AGENDA

Ninth (9th) Meeting of SENATE of

Indraprastha Institute of Information Technology, Delhi

Date: 29th January 2010

Day: Friday

Time: 3.00 PM

Venue: Conference Room
3rd Floor, Library Bldg
NSIT Campus
Dwarka, Sector - 3
New Delhi

NINTH (9TH) MEETING OF SENATE OF IIIT-DELHI

INDEX

Sl. No	Description			Page No
1.	**Agenda Items**			
	9.0 Chairman's opening remarks			1
	9.1 Confirmation of minutes of the 8th meeting of Senate			1
	9.2 M Tech program in Computer Science			1
	9.3 Courses in Security Programs			1
	9.4 Any other items with permission of Chair			1
2.	**Annexure No.**		**Item No.**	
	Annexure 1	–	9.1	
	Annexure 2	–	9.2	
	Annexure 3	–	9.3	

NINTH (9TH) MEETING OF SENATE OF IIIT-DELHI

AGENDA

9.0 Opening remarks of Chairman

9.1 Confirmation of minutes of the 8th Senate meeting. *(Also confirmed through circulation by majority)* ***(Annexure 1)***

9.2 M. Tech Program in Computer Science ***(Annexure 2)***

9.3 Courses in Security Program ***(Annexure 3)***

9.4 Any other matter with the permission of Chair

****

Annexure 1

Minutes of the 8th Senate Meeting of IIIT-D held on January 6th 2010, at 3.30 PM in Conference Room, Library Building, IIIT Delhi.

Following members were present:

- Prof. Pankaj Jalote, (Chairman)
- Dr. Astrid Kiehn
- Dr. Vikram Goyal
- Dr. Veena Bansal
- Dr. Ashish Sureka
- Dr. Ponnurangam Kumaraguru
- Dr. Amarjeet Singh
- Dr. Pushpendra Singh
- Dr. Somitra Sanadhya
- Dr. K. K. Biswas
- Dr. A. R. Subramanian (Secretary)

Members present through Audio Conferencing:

- Mr. Saugat Sen, Cadence
- Mr. Pawan Goyal, Adobe Systems

8.0 Opening remarks of Chairman

The Chairman extended a warm welcome to all those who were present in person as also to those on audio-conferencing.

8.1 Confirmation of minutes of the 7th Senate meeting.

As there were no comments, the minutes were confirmed.

8.2 Appeals by students

Prof Astrid Kiehn briefed the members with the following inputs:

First year students' appeals:

17 first year students failed in one or more courses in Monsoon Semester 2009:

- Four students failed in three courses (DM, IP, DC)
- Five students failed in two courses (4 in DM and DC,1 in DM & IP)
- Nine students failed in one course (3 in DM, 6 in DC)

All these students had appealed for being allowed to register for CO and TOC which require passing of the courses DC and DM, respectively, as a prerequisite. The students who had failed two courses can only proceed to the third semester if they clear all the courses offered (UG guidelines, Sect. 8.1). Otherwise they would not be able to earn more than 22 credits as required.

Second year students' appeals:

There are 12 students who have a backlog from the second semester, that is they have to clear either CO or TOC (11 students) or both of the courses (1 student, only). Most of them had requested for an overload that is to register for the entire course that were scheduled for the 4th semester and additionally for CO or TOC. The timetable would have allowed them to do that without over lapping. Apart from the two students under academic warning they had cleared all the courses of the third semester.

After considering the appeals and facts, the senate decided the following:

- All first-year students may register for all the courses offered / scheduled for the second semester. They must submit a letter stating that they will work extra & that they take full responsibilities.

- No overload will be granted to any second-year student beyond than five, 4-credit courses (total 20 credits). The senate observed that the word “overload” has not clearly been defined yet and that that had to be done soon.
- The TOC/CO backlog does not need to be cleared this semester.

Some foundation courses in which there are many backlog may be offered during summer in the next two years.

8.3 M. Tech Program

The Senate considered the Note on the M.Tech program scheduled for the forthcoming academic session of 2010-11.

8.4 Courses offered in the Winter Semester 2010

The Senate noted the courses offered in the Winter Semester as circulated.

8.5 Any other matter with the permission of Chair

- The 75% attendance requirement as per UG Manual shall be enforced (i.e less than 75% of attendance implies failure in the course). In the last semester it had not been applied as the students had not known about this rule from the beginning of the semester.

- As fee for late academic registration a student has to donate a book to the library worth around Rs 300/-.

There being no other items, the meeting ended with vote of thanks to the Chair.

****

Annexure 2

MTech in Computer Science @ IIIT-Delhi

1 Background

IIIT-Delhi subscribes to the view that a Masters degree is primarily industry-focused, though it can be used as a stepping stone for research as well. And the decision whether the degree is to be pursued for skill and knowledge up-gradation or also for building research skills should rest with the student. In addition, the Institute believes that a student should also be given a choice of pursuing MTech (full time) without assistantship or with assistantship (i.e. financial support in-lieu of some academic work). Doing MTech without assistantship can allow a student to finish the MTech sooner, since the student does not have to do any part-time work, as required when the student is receiving an assistantship.

Furthermore the Institute wants to provide specializations within Computer Science in its MTech program. There is today a greater need for specialized manpower in industry as each field gets larger and more complex. With specialization, the Institute plans to develop highly skilled manpower in some focus areas where there is a need in the industry. (Technology companies that IIIT-Delhi surveyed also endorsed and appreciated the view of specialized MTechs.)

The rules and regulations of the general MTech program in IIIT-Delhi are given in the PG manual of the Institute. This document specifies the requirements for the "MTech in Computer Science" program. In this program, a student has the option of doing "MTech in Computer Science with specialization in <area>".

2 Requirements

Overall Requirements

MTech in Computer Science may be done at IIIT-Delhi (1) with a thesis or (2) without a thesis but with a scholarly paper. In both options, students have to do certain amount of course work. In addition, students doing MTech *with thesis* will have to do a thesis. Students in MTech *without thesis* have to do more courses, but instead of a thesis they have to do a scholarly paper. The overall requirements are as follows:

1. **MTech with thesis.** 32 units of course work + 20 units of thesis. At most 4 units may be earned by doing 300 and 400 level courses – rest must be at 500 level and above.

2. **MTech without thesis .** 40 units of course work + 12 units for a scholarly paper. At most 8 units may be earned through doing 300 and 400 level courses.

Hence, the total credit requirement for a MTech is 52 units. For thesis or scholarly paper units, though the student has to register, he/she need not be physically present and can do the work while being outside the Institute. (A regular, semester course is 4 units.)

A student admitted to the MTech program can decide at any time during the program which of the two options he/she wants. Generally, however, it is expected that the student will decide by the end of the first semester which option he/she wants to pursue. The option can be changed later, if the student wishes.

Core Courses

Each student has to do a set of "core courses" which provide advanced, but foundational, training in computer science. A student is expected to take 12 units as part of the core. The core comprises of one course each from the following groups:

- Algorithms/theory: {Advanced algorithms, Theory, …}
- Systems: {Distributed computing systems, Advanced operating systems,..}
- Software: {Software tools and techniques, Secure programming, …}

[QUESTION: Should we add a communication skills course as compulsory? This can be the technical communication course offered in 3rd year of the UG program – these students can join that class.]

[QUESTION: Should we have a "minor project" as a compulsory course, like it is in IIT Delhi. This will ensure that everyone, even a non-thesis option student, does a small project – a project is expected to be evaluation oriented. This reduces the number of courses, but increases the project load on faculty and these projects may not necessarily result in anything useful. From teaching perspective, this may be of limited value if we ensure that there are projects in courses. It can be useful for with-thesis option – to reduce the course load by one.

Electives

All other courses are electives and students can chose which courses he/she wishes to do to complete the requirements of the MTech. At most 4 units of "Independent Study" and 4 units of "Minor Project" can be taken.

Requirement for Specialization

For pecializing in an area, from among the areas in which specializations are offered by the Institute, the student must do at least 16 units (excluding the thesis units) of courses in that area, and must do his/her thesis units in that area. (The advisor will certify this). (If a course is in the list of courses for a specialization, as well as in one of the groups for core

courses, that course can be used for satisfying both the core and specialization requirements. However, the overall requirements remain unchanged.)

The lists of courses for each specialization are specified separately. (Currently, the Institute is planning to start a MTech with specialization in ***Information Security***; other specializations will be added gradually over the next few years.)

While it is possible to do a MTech without specialization, the Institute encourages all students to specialize.

3 With or Without Assistantship

Limited number of Assistantships will be available for MTech students. A student who is offered an Assistantship will be required to do some academic work in-lieu of the Assistantship. Assistantship is available only for *with*-thesis option.

As per the PG manual, the normal load for a student without assistantship is 20 units,. Hence, ***a student with Assistantship will require four semesters to finish the program*** (in three semesters the max units a student can do is 48). A student without assistantship can, however, finish the program in 3 semesters, as the student can take a higher load since he/she does not have to spend time doing assistantship work. Some sample schedules for various options are given below:

- **Schedule A (without Assistantship, without thesis)**:
  - Sem I: 20 unit course work
  - Sem II: 20 units course work
  - Summer: Internship
  - Sem III: 12 units of scholarly paper

- **Schedule B (without Assistantship, without thesis):**
  - Sem I: 20 units course work
  - Sem II: 20 units course work
  - Summer: 4 units of scholarly paper
  - Sem III: 8 units of scholarly paper (which can be done while working elsewhere)

- **Schedule C (without Assistantship, with thesis)**:
  - Sem I: 20 unit course work
  - Sem II: 12 units course work + 8 units of thesis
  - Summer: Internship or 4 units of thesis
  - Sem III: 8 or 12 units of thesis

- **Schedule D (with Assistantship, with thesis):**
  - Sem I: 16 units course work
  - Sem II: 12 units course work + 4 units of thesis
  - Summer: Internship or Assistantship work

- Sem III: 4 units course work and 8 units of thesis
- Sem IV: 8 units of thesis

Schedule D is what a typical student in this category (with Assistantship, with thesis) will follow in an IIT. This schedule as well as the overall duration is essentially same as what is followed in IITs, which only offer this category. In this sense, the proposed MTech program is consistent with the MTech program in IITs.

Annexure 3

Courses in the M. Tech. Program (Initial Draft)

Information security is a key concern in the world today. It is also a very complex area, which requires well trained people. In India, there are few PG programs in Information Security, and almost none which are technically solid.

The main aim of the program is to produce highly trained manpower which can develop secure applications, make an IT infrastructure secure, and monitor and analyze security of a system. The main goal is to produce manpower that will be highly sought after by industry, but which is also ready to do research in the area, should the student chose that path. So, the primary focuses of the M.Tech. Program in IIIT-Delhi will be on technology, though there will be some modules on policy as well.

The M.Tech. Program in IIIT-D (which is getting finalized) will require 9 or 10 courses in the without-thesis option and about 7 courses in the with-thesis option.

This is a very initial draft to get the discussion going. It borrows heavily from CMU program. Most of the courses will involve hands-on projects and programming exercises. A student is supposed to do all foundation courses.

FOUNDATION COURSES

Foundation courses for security – those courses that most of the students in this program are expected to do. It should be remembered that the intake in this program are students who are expected to have a decent CS background.

The foundation can consist of three courses – one on developing secure software, one about how modern distributed systems are structured and organized as most of the source of security problems are due to the distributed nature of the systems today, and the third course on introduction to security.

Modern Distributed Systems

Build upon the basic computer network knowledge to cover topics like flow control, firewalls, internetworking, intranet and internet, major components in a networked system, various advanced protocols – ssh, payment, etc. Why networks are designed they way they are, designing networks, etc.

In addition, it will also cover fundamental principles underlying distributed systems, and cover topics like models of distributed systems, distributed transactions, distributed filesystems, infrastructures for building distributed systems, distributed algorithms and applications, overview of distributed multimedia applications.

Foundations to Computer Security

This course provides a principled introduction to techniques for defending against hostile adversaries in modern computer systems and computer networks. Topics covered in the course

include operating system security; network security, including cryptography and cryptographic protocols, firewalls, and network denial-of-service attacks and defenses; user authentication technologies; security for network servers; web security; and security for mobile code technologies, such as Java and Javascript. More advanced topics will additionally be covered as time permits, such as: intrusion detection; techniques to provide privacy in Internet applications; and protecting digital content (music, video, software) from unintended use.

Secure Software Systems

Poor software design and engineering are the root causes of most security vulnerabilities in deployed systems today. Moreover, with code mobility now commonplace – particularly inthe context of web technologies and digital rights management – system designers are increasingly faced with protecting hosts from foreign software and protecting software from foreign hosts running it. This class takes a close look at software as a mechanism for attack, as a tool for protecting resources, and as a resource to be defended. Topics covered include the software design process; choices of programming languages, operating systems, databases and distributed object platforms for building secure systems; common software vulnerabilities, such as buffer overflows and race conditions; auditing software; proving properties of software; software and data watermarking; code obfuscation; tamper resistant software; and the benefits of open and closed source development.

Advanced Algorthims

Knowing advanced CS algorithms is an absolute necessity for the M.Tech in CS; this course is meant to be a refresher and enabler for advanced topic on algorithsm. Some topics to cover in this course are: DFS, BFS; heaps, binomial and fibonacci heaps; amortized analysis; splay trees; self-organizing data structures; random search trees; plane and planar graphs; plane, planar graph, planarity testing algorithm; reduction and NP complete problems; approximation algorithms; probability and randomness; random walks and graphs; linear programming; parallel algorithms; competitive algorithms;

ELECTIVES

Rest of the courses in this stream are all electives, focusing on different aspects of security. A student can chose to do any set of courses from this to satisfy his/her course requirement. The set of electives will change with time. A suggested initial list is given below.

Network Security

Some of today's most damaging attacks on computer systems involve the exploitation of network infrastructure, either as the target of attack or as a vehicle to advance attacks on end systems. This course provides an in-depth study of network attack techniques and methods to defend against them. Topics include firewalls and virtual private networks; network intrusion detection; denial of service (DoS) and distributed denial-of-service (DDoS) attacks; DoS and DDoS detection and reaction; worm and virus propagation; tracing the source of attacks; traffic analysis; techniques for hiding the source or destination of network traffic; secure routing protocols; protocol scrubbing; and advanced techniques for reacting to network attacks. Offered in the Spring. Prerequisites: Foundations to Computer Security.

Wireless Security

Wireless networks have some unique problems for security. This course will cover the problems in security in wireless systems, and how to make such systems secure. Some topics to cover: understanding the threats on the wireless networks – rogue access points, DoS and eavesdropping; security measures in WEP, WPA/WPA2, 802.11; auditing wireless network. [If there is much overlap with network security, then this may also include security in mobile &/or sensor networks]

Applied Cryptography

A wide array of communication and data protections employ cryptographic mechanisms. This course explores modern cryptographic (code making) and cryptanalytic (code breaking) techniques in detail. This course emphasizes how cryptographic mechanisms can be effectively used within larger security systems, and the dramatic ways in which cryptographic mechanisms can fall vulnerable to cryptanalysis in deployed systems. Topics covered include cryptographic primitives such as symmetric encryption, public key encryption, digital signatures, and message authentication codes; cryptographic protocols, such as key exchange, remote user authentication, and interactive proofs; cryptanalysis of cryptographic primitives and protocols, such as by side-channel attacks, differential cryptanalysis, or replay attacks; and cryptanalytic techniques on deployed systems, such as memory remanence, timing attacks, and differential power analysis.

Digital Forensics

Society has just started to cultivate the legitimate and the beneficial potential of the rapidly changing and extremely powerful digital technology for business, empowering individuals & communities and for promoting economic development. World cultures are becoming more and more dependent on digital computer systems and networks. Criminals are exploiting digital technology to assist in committing traditional as well as innovative forms of unpredictable and unforeseen crimes. This course concentrates on providing introduction to computer frauds and cyber crimes and a systematic introduction to the field of digital forensics. The course aims to familiarize students with the forensic process and to apply forensic principles with many tools of the trade. This course will introduce students to the foundations of digital forensics. Students will also get some hands experience on various topics through assignments, and project.

Cyber Forensics

This course concentrates on providing introduction to cyber crime and on the collection and analysis of evidence left on the cyber world. Upon completion of this course, a student will feel comfortable with the full scope of a cyber forensic investigation. Class periods will consist of lecture and exercise. Students will learn about the data types that may have forensic value; and will be introduced to several techniques for capturing data off the network and how each option impacts the data that is available. Students will be further presented with several incident response challenges on live networks and be tasked with determining and proving what happened. They will have to collect various logs, network traffic, create timelines, and draw conclusions.

Human Aspects of Information Security

With the rise of the Internet as a major mode for economic transactions and communication, online trust, and cyber crimes have increasingly become an important area of study in computer

science, public policy and business. Today, individuals often do not know whether to trust an online merchant with their personal information or whether the emails they receive come from legitimate entities. Because of the increasing sophistication and volume of cyber attacks, Internet users are making incorrect decisions that cause significant economic damage to themselves and enterprises. As a result, developing technologies that help users make better online trust decisions has become important. This course will motivate the necessity for more work in the area of usable privacy and security. Particularly, will also focus on how these usable privacy and security issues are relevant to a developing nation like India and how we can address these issues.

Other electvies that we are planning offer

Anonymity and Privacy

This course will focus on how to keep data (residing in databases or otherwise) secure. And also how to preserve the privacy of such data. Other topics to be covered: identifiability of data; data profiling; data fusion; data anonymity; de-identification; k-anonymity; privacy preserving data mining techniques.

Economics of Information Security

This course will address questions like – Who are the stakeholders in the information security landscape? Who has the incentive to solve the information security problems? What are the solutions that we can develop to build a more secure online enviroment keeping the constraints among various stakeholders?

Managing Security

Policy, risk analysis, monitoring, threat analysis, etc. This course will also focus on various security standards – ISO 27001, COBIT, etc. This could be broken into a few 2-unit courses on policy, risk analysis, etc.

Ethical Hacking / Penetration Testing

Sample topics that will be covered in this course: offensive sniffing; breaking IP based ACLs; evidence remoal (anti-forensics); hacking web applications; cross site scripting; Unix, windows, and routers password cracking; buffer overflow exploit.

Critical Infrastructure Protection (CIP)

Sample topics to be covered: What is criticial infrastructure? – Power generation and distribution, water systems, and communications; disaster recovery; threat analysis and modeling; CIP laws and policies; physical, computer, personnel, operations, and data security.

Biometrics and security

Sample topics to be covered: Surveillance and monitoring; finger printing; iris and voice recognition; retina scanning; multimodal biometrics; cancelable biometrics; biometric standards; privacy issues in biometrics;