CS 6500: Network Security

Odd Semester: Jul.-Nov. 2025
L Slot: Thu. 2:00PM–3:15PM ; Fri. 3:30PM–4:45PM
Prof. Krishna Sivalingam, SSB 313; Phone: 4378
Email: *skrishnam@cse.iitm.ac.in, krishna.sivalingam@gmail.com*
Teaching Assistant(s): TBA
URL: `http://courses.iitm.ac.in/` (Moodle Site)

1 Course objectives

The objective of this course is to teach the concepts of securing computer network protocols and network communications, based on the application of cryptography techniques.

2 Course credit structure

The course credits are: Lecture(3) + Practice (6) + Other (3), for a total of 12 hours per week. The programming assignments and term project are expected to take on average, around 6 hours per week.

3 Course prerequisite(s)

Strictly Enforced: CS2700/CS2710 (Programming and Data Structures) and CS3200+CS3210 / CS3205 (Computer Networks Theory and Lab), or equivalent courses as approved by the instructor.

Required: The student must also have strong programming abilities in one or more of C/C++/Java/Python languages.

Note: *The prerequisite of CS6530 (Applied Cryptography) is being waived this semester, since it has not been taught in the CSE Dept. for the past few years.*

4 Required Textbooks

STAL Cryptography and Network Security: Principles and Practice, William Stallings; `http://williamstallings.com/Cryptography/`, Seventh or Later Edition.

NS Network Security Essentials, Sixth or Later Edition, W. Stallings. `http://williamstallings.com/NetworkSecurity/`

5 Reference Textbooks/Others

Most network textbooks seem to be revised every 1-3 years; hence, please refer to the latest revision.

STEW Network Security, Firewalls And VPNs, J. Michael Stewart, Jones & Bartlett Learning, 2013, ISBN-10: 1284031675, ISBN-13: 978-1284031676.

GREG The Network Security Test Lab: A Step-By-Step Guide, Michael Gregg, Dreamtech Press, 2015, ISBN-10: 8126558148, ISBN-13: 978-8126558148.

YANG Herong Yang, "Cryptography Tutorials - Herong's Tutorial Examples", `http://www.herongyang.com/Cryptography/`, 2017.

In addition, recent research articles on Network Security may also be used. If you see other good reference books, please email me.

6 Course Requirements

You are *required* to attend all the lectures. If you miss any of them it is your responsibility to find out what went on during the classes and to collect any materials that may be handed out.

Course related announcements will be made in class (primarily), via Google Classroom and IITM Moodle, and occasionally by email to your IITM mail ID. It is your responsibility to monitor/forward your IITM email

accounts regularly; please check your 'smail' IDs at least once daily, if not more often.

Minimum attendance of 85% is required; else, a 'W' grade will be reported.

Class participation is strongly encouraged to demonstrate an appropriate level of understanding of the material being discussed in the class. Regular feedback from the class regarding the lectures will be very much appreciated.

All individual assignments must be done individually! Group assignments must be done only by students of that group! Suitable action will be taken, as per IITM policy, in case of any type of code-sharing, downloaded-code submission and other forms of academic dishonesty, in the assignments and exams.

7 Planned Syllabus

The following topics will be covered, but not necessarily in the order listed below:

Basics of cryptography: symmetric and public-key cryptography, hash functions, MAC, authentication, and digital signatures. hrs)

Key Management and Distribution: Symmetric Key Distribution, Distribution of Public Keys, X.509 Certificates, Public-Key Infrastructure.

User Authentication: Remote User-Authentication Principles, Remote User-Authentication Using Symmetric Encryption, Kerberos Systems, Remote User Authentication Using Asymmetric Encryption.

Transport-Level Security: Web Security Considerations, Secure Sockets Layer / Transport Layer Security, HTTPS standard, Secure Shell (SSH) application.

IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange (IKE), Virtual Private Networks (VPNs).

Electronic Mail Security: Pretty Good Privacy, S/MIME, DomainKeys Identified Mail.

Wireless Network Security: Mobile Device Security, IEEE 802.11i Wireless LAN Security.

Network Access Control: Network Access Control, Extensible Authentication Protocol, IEEE 802.1X Port-Based Network Access Control.

Firewalls and Intrusion Detection Systems: Packet Filtering, Intrusion Detection, Firewall Characteristics, Types of Firewalls, Deep-packet Inspection, ML Techniques.

Some advanced topics: (Time permitting) Blockchain, IoT Security and other recent topics; Recent research articles on network attacks, detection and attack handling mechanisms.

8 Tentative Grading Policy

The following allocation of points is tentative. These may change during the semester.

Component	Weight
Midterm Test (TBA):	20%
Final Exam (TBA):	35%
Programming Assignments (3 – 4):	25-30%
Term Project (as a Team of 1–2 students):	15-20%

There will be 3–4 programming assignments involving the use of tools, libraries and packages such as Wireshark, OpenSSL and Snort. These will be given approximately 2–3 weeks from announcement to submission.

There will be a Term Project, which will be done as a team of 1–2 members. The specific problem will be determined by the team members; with the project proposal submitted mid-semester. This can be based on a new research idea or an implementation of an existing work/protocol. This will be given approximately 4–5 weeks from proposal acceptance to submission.

To obtain a pass grade, the student must score at least 30% in the programming assignments (overall), at least 30% in the quiz/exams (combined).

9 Other Policies

- Attendance will be noted for online classes, based on screenshots taken by the TAs every 20 minutes.

  Students who are not able to attend a given lecture due to network/system problems MUST fill out an attendance waiver request form, within 24 hours except under extenuating circumstances.

- Since this is an elective, there will be NO supplementary final exam, in case a student receives the 'U' grade.

- All assignments must be submitted by the respective deadlines. Late submissions (esp. bunched submissions at the end of the semester) will not be considered.

- **NO sharing of code between students, submission of downloaded code (from the Internet, Campus LAN, or anywhere else) is allowed.** Students who violate the Academic Honor Code will be reported to the IITM Senate-appointed Students Discipline and Welfare Committee, for necessary action.

- **Absolute adherence to policies regarding conduct during online Midterm/Exam is required.** Students who violate the Academic Honor Code will be reported to the IITM Senate-appointed Students Discipline and Welfare Committee, for necessary action.

- **Please protect your Moodle account or Google account password. Do not share it with ANYONE. Do not share your academic disk drive space on the Campus LAN or on the Cloud such as Google Drive (ClassRoom), Dropbox, Github, etc.**