Course Handout

CS 402 Network Security

Autumn Semester, 2025

Department of Computer Science and Engineering

National Institute of Technology Warangal

Course Website:https://classroom.google.com/c/Nzg5MjA0OTIyNTAz

1. Objectives:

The course offers a blend of theoretical and practical elements, focusing on the foundational principles and developments in network security. It aims to elucidate core concepts and insights essential for understanding and mitigating various network security threats and vulnerabilities. The course encompasses precise analytical models and detailed performance analysis for different network security mechanisms. Key topics include user authentication, malicious software, IP security, and application-level threats, with an emphasis on technologies such as symmetric and asymmetric encryption, firewalls, and intrusion detection systems. The course also lays groundwork for advanced security techniques, including blockchain and web-based malware defense. A significant component involves hands-on programming assignments using tools like Wireshark, OpenSSL, and Snort to analyze network vulnerabilities and attacks.

2. Prerequisites:

Computer Networks, Cyptography course from the CSE department.
Students are expected to be familiar with basic concepts of Computer Networks and Cryptography. Topics include

- TCP / IP stack, Internet Protocol, TCP handshake, Routing and congestion control algorithms
- Symmetric key encryption techniques, public key cryptography, digital signatures

3. Course Contents:

Topic	No of Lectures
Review of the prerequisites	**2**
User Authentication	
User Authentication, Remote User-Authentication Principles	1

Remote User-Authentication Using Symmetric Encryption	2
Kerberos Systems, Remote User Authentication Using Asymmetric Encryption	3
Remote User Authentication Using Asymmetric Encryption	1
IP Security	
IP Security Overview, IP Security Policy	1
Encapsulating Security Payload	2
Combining Security Associations	1
Internet Key Exchange (IKE)	1
Transport-Level Security	
DNS, Web Security Considerations	1
Secure Sockets Layer, Transport Layer Security	2
Transport Layer Security, HTTPS standard, Secure Shell (SSH) application, Electronic Mail Security- Pretty Good Privacy, Analysing and defending against web-based malware.	3
Malicious Software	
Viruses, Worms, System Corruption, Attack Agents, Information Theft, Phishing	1
Spyware Payload Stealthing, Backdoors, Rootkits, Distributed Denial of Service Attacks	1
DoS Attacks and Network Defenses	
DoS Attacks and Network Defenses, Network Access Control	1
Extensible Authentication Protocol, IEEE 802.1X Port-Based Network Access Control	1
IEEE 802.1X Port-Based Network Access Control	1
Firewalls and Intrusion Detection Systems	
Firewalls and Intrusion Detection Systems, Types of Firewalls, Firewall Basing, Firewall Location and Configurations	1
Overview of Blockchain	2

4. **Special Emphasis:**
    - Deployment / setup of software, firewall rules
    - Authentication protocols
    - Network attacks and countermeasures

5. **Lecture, Tutorial & Lab Schedule & Venue:**
    - Venue: C303
    - Timings:

      Monday – 15:00 – 16:00
      Tuesday – 16:00 – 17:00

6. **Office Hours or, recommended mode of contact beyond formal contact hours:**
    - Students can contact both instructor as well as TAs via e-mail.
    - Can meet in-person in the office

7. **Evaluation Components & Policies:**

Exam	Weightage
Mid-Sem	30%
End-Sem	40%
Laboratory	30%

Exam/ Assignment/ Term Paper Policy: If a student misses any Mid-sem, marks will be pro-rated based on remaining ones, if valid reason is provided along with supporting documents. If a student misses the end-sem exam, he/she can apply for makeup examination. Assignment submission is due by 12 Noon of respective due date. 15% Marks will be deducted for late submission. No makeup or prorating will be done for missed assignment submissions.

8. **Course Policies: Attendance, Honesty Practices, Withdrawal (within the limits of DOAA Guidelines)**

Attendance Policy: Minimum 80% attendance. Attendance will be recorded in every session. Each student is expected to take notes

9. Books & References: Properly Formatted along with listing of possible internet sources.

Text Book	
Cryptography and Network Security: Principles and Practice	William Stallings, 8th Edition, 2023, Pearson, e-ISBN:978-1-292-43749-1
Network Security: Private Communications in a Public World	M. Speciner, R. Perlman, C. Kaufman Prentice Hall, 2002.

Online References for certain topics, including slides will be provided during the course.

10. Instructor and TA Information

Instructor	
Prof. Sriram Kailasam	**Dept. of CSE, Cluster 1, CS 131** **e-mail: sriramk@nitw.ac.in** **Ph: 2722**
Prof. Suresh Babu	**esbabu@nitw.ac.in**
Course TAs	
Shruthi K	
Anusha	