CS 4310: COMPUTER AND NETWORK SECURITY

Semester Hours:	3.0	*Contact Hours:* 3
Coordinator:	Ruinian Li	
Text:	Readings provided by instructor	
Author(s):	VARIED	
Year:	Varied	

SPECIFIC COURSE INFORMATION

Catalog Description:

Cryptographic techniques, including hashing, key distribution, and authentication; Comprehensive study of security protocols such as IPsec, SSH, VPN and TLS; Attacks and defenses in remote access, web applications and wireless networks; Hands-on experience with penetration testing, data protection with cryptographic algorithms in secure applications; security implications of emerging technologies. Prerequisites: a grade of C or better in CS 2310 or CS 3320, and a corequisite of CS 4390.

Course type: **ELECTIVE**

SPECIFIC COURSE GOALS

- I can compare common authentication schemes. (Analyze)
- I can analyze common security protocols in network communication. (Analyze)
- I can assess defense mechanisms for common web attacks. (Evaluate)
- I can assess defense mechanisms for common wireless attacks. (Evaluate)
- I can utilize common penetration tests. (Apply)
- I can evaluate cryptographic algorithms to protect data privacy in online applications. (Evaluate)

LIST OF TOPICS COVERED

- **Introduction to Computer and Network Security** (~7%)
    - Overview of basic network protocols

    - Understanding malwares and their types
    - Role and functionality of security gateways
    - Denial of service attacks and mitigation techniques
- **Cryptography Fundamentals** (~10%)
    - Computational difficulty in cryptography
    - Random numbers
    - Security foundation of symmetric/asymmetric encryption algorithms
    - Cryptographic hashes: password hashing, commitment schemes, Merkle trees
- **Authentication** (~7%)
    - Password-based authentication
    - Address-based authentication
    - Biometrics in authentication
    - Key distribution and recovery
- **Remote Access Attacks and Defenses** (~10%)
    - Transport layer security (TLS)
    - IPsec, IKE (Internet Key Exchange Protocol)
    - SSH authentication and tunneling mechanisms
    - VPN and anonymous communication
- **Web Attacks and Defenses** (~18%)
    - Cross-Site scripting and defenses
    - Cross-Site request forgery and defenses
    - Injection attacks and defenses
    - DNS attacks and defenses
- **Wireless Attacks and Defenses** (~10%)
    - Packet sniffing and spoofing, and defenses
    - Jamming Attacks and defenses
- **Penetration Testing and Security Assessments** (~14%)
    - Basic penetration testing techniques and tools
    - Social engineering attacks and human factors in security
    - Practical security assessment methodologies
- **Cryptographic Techniques for Data Protection** (~7%)
    - Proxy-based re-encryption scheme
    - Identity-based and attribute-based encryption
    - Homomorphic encryption, secret sharing, and zero-knowledge proof
- **Blockchain** (~7%)
    - Introduction to Bitcoin and Ethereum
    - Decentralized identifiers (DIDs) and their role
- **Machine Learning and Security** (~7%)
    - Adversarial examples in machine learning
    - Generative adversarial networks (GANs)
    - Machine learning techniques for security analytics
- **Security for Emerging Network Technologies:** (~7%)
    - 5G security considerations
    - IoT network security challenges
    - Edge computing and its implications for network security