Dept Number	CS 410	Course Title	Computer Security
Semester Hours	3	Course Coordinator	Kemal Akkaya
Catalog Description	A broad overview of the principles, mechanisms, and implementations of computer security. Topics include cryptography, access control, software security and malicious code, trusted systems, network security and electronic commerce, audit and monitoring, risk management and disaster recovery, military security and information warfare, physical security, privacy and copyrights, and legal issues.		

Textbooks

Stallings, William. *Cryptography and Network Security: Principles and Practice.* Prentice Hall, 6th Edition, 2012. ISBN: 9780133354690.

References

- Pfleeger, Charles and Shari Pfleeger. *Security in Computing.* Prentice Hall, 4th Edition, 2007.
- Bishop, Matt. *Introduction to Computer Security*. Addison Wesley, 1st Edition, 2005.
- Gollmann, Dieter. *Computer Security*. John Wiley & Sons, 2nd Edition, 2006.
- Kaufman, Charlie, Radia Perlman and Mike Speciner. *Network Security: Private Communication in a Public World*. Prentice Hall, 2nd Edition, 2003.

Course Learning Outcomes

- To learn the principles, mechanisms and implementation of information and communication security in computer systems and networks.
- Understand the fundamentals of cryptography and its deployment.
- To learn the up-to-date security protocols and explain the design criteria and possible flaws behind them.
- Understand the security threats and their countermeasures.
- To learn to build secure software and systems.
- To learn programming techniques for security protocols.

Assessment of the Contribution to Program Outcomes

Outcome →	1	2	3	4	5	6	7	8	9	10
Assessed →	X	X	X		X		X	X		

Prerequisites by Topic

306 with a grade of *C* or better.

Major Topics Covered in the Course

1. Introduction: security goals, types of threats, security policies models, security standards {2 classes}
2. Cryptography: classical ciphers stream and block ciphers, public-key encryption, hashes and message digests, signature schemes, key establishment and management {12 classes}
3. Network security: PKI, E-mail security, IP security, Web security, virtual private networks, sniffing and spoofing, firewalls, denial-of-service attacks, electronic commerce wireless security {11 classes}
4. System security: access control, authentication and authorization, file protection, intrusion detection, trusted computing and digital rights management, UNIX security {8 classes}
5. Program security: buffer overflow attacks, viruses and worms, Trojan horses, proof-carrying code, sandboxing, Java security {4 classes}
6. Physical security, operational security, ethical and legal issues in security {5 classes}