



# CENG 374E - INTRODUCTION TO COMPUTER SECURITY

**Prof. Dr. Şeref SAĞIROĞLU**

Gazi University  
Engineering Faculty  
Computer Engineering Department  
Maltepe/Ankara

[SS@gazi.edu.tr](mailto:ss@gazi.edu.tr)

<https://avesis.gazi.edu.tr/ss>

# **CENG 374E - INTRODUCTION TO COMPUTER SECURITY**

## **COURSE OUTLINE & INTRODUCTION**





# Who am I?

**Prof. Dr. Seref SAGIROGLU**

**PhD:** Cardiff University, School of Engineering, 1994

**Work Experience:** Erciyes University, Gazi University

**Other Experience:** Cardiff University, Sheffield University,



# Who am I?

**Prof. Dr. Seref SAGIROGLU**

**Research Interests:** Robotics; Biometrics; Intelligent System Identification, Modelling and Control; Artificial Neural Networks and Applications; Network and Information Security, Cyber Security, Big Data Analytics, AI, Generative AI

**Contact:** [ss@gazi.edu.tr](mailto:ss@gazi.edu.tr)

**Office hours:** by appointment (Room 124) send me an email.



# Teaching Assistant

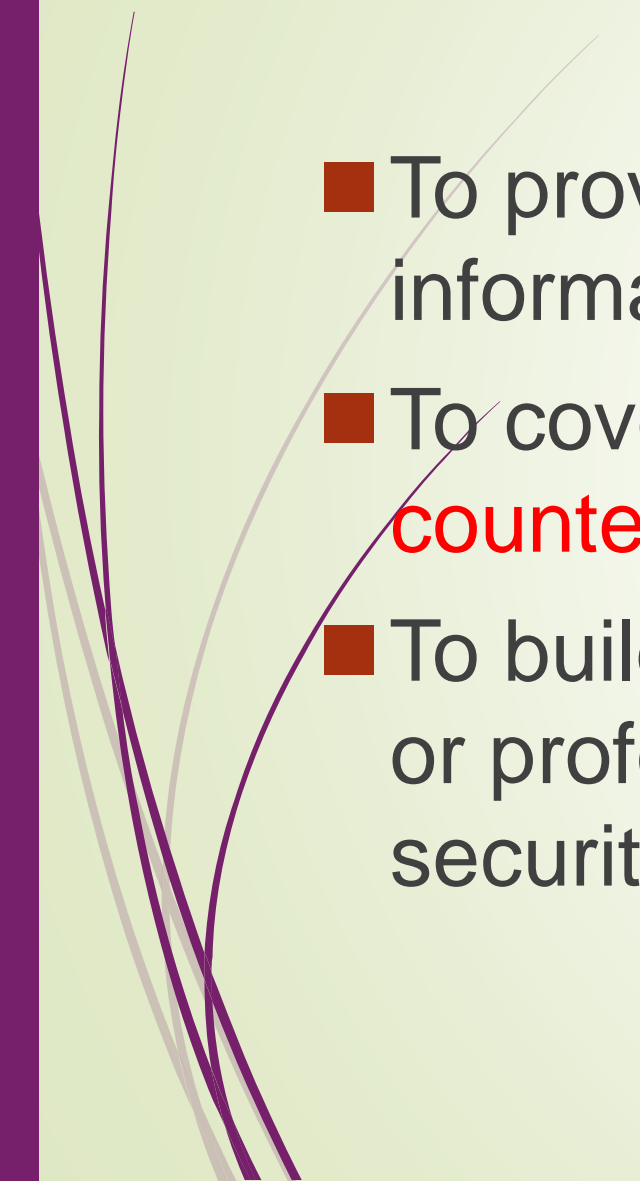
**Res. Asst.: ?**

**Contact. : ?**



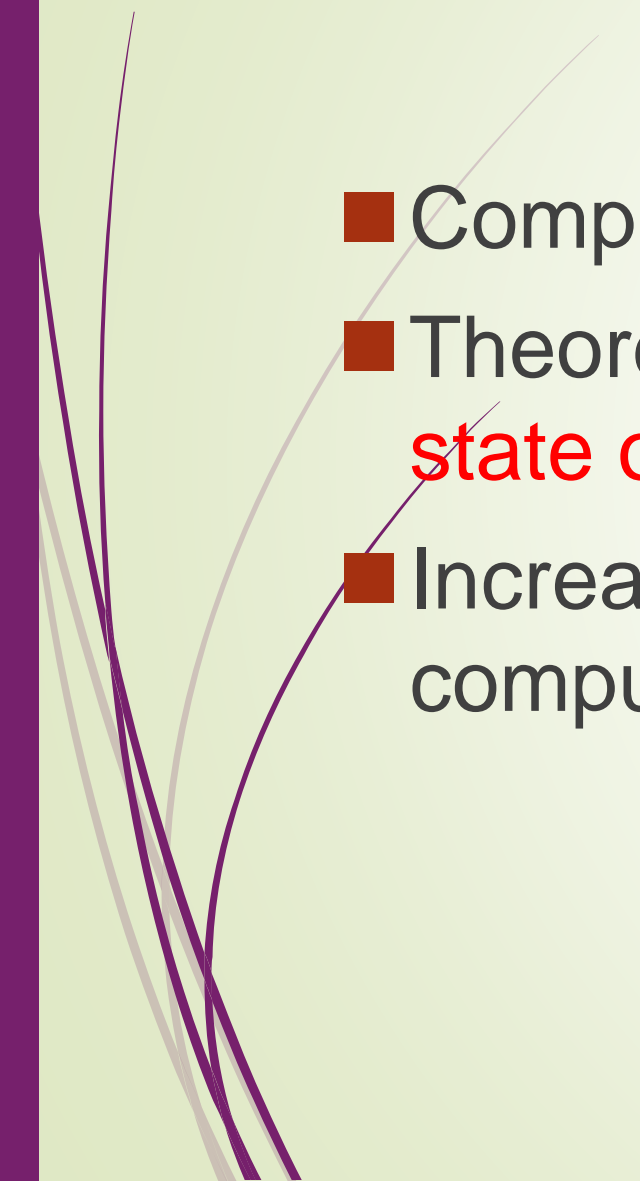


# Course Outcome

- To provide an introduction to computer and information security topics
  - To cover various security **threats** and **countermeasures**
  - To build a foundation for future academic research or professional work on computer and information security
- 



# Course Outcome

- Computer and information security **literacy**
  - Theoretical and practical knowledge about the **state of the art** and **trends** in computer security
  - Increased **awareness** about how to ensure computer security
- 



# Some of Resources

No textbook is required, but the following will be useful:

- "Security Engineering", R. Anderson, 0-471-38922-6, Wiley, New York, 2001.
- "Cryptography And Network Security Principles And Practices", W. Stallings, 0-13-091429-0, Prentice Hall, 2003.
- "Security in Computing", Charles R. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2006.
- Academic articles
- Large Language Models



# Grades

## MIDTERM (MT)

- 5 homeworks / assignments (at least) = 50%
- 1 midterm exam = 50%

## FINAL EXAM (FE)

- 1 Exam = 40%
- 1 Project Report + Presentation = 60% (40%+20%)



# Assignments



- Submissions will be made via drive account.
- There will be mathematical problems, proofs, coding etc.
- If the assignment involves coding, submissions will be made via email to the TA.

# Assignments


- Can be a **detailed survey** on an advanced topic
- Can be an **implementation** of a security algorithm /protocol /architecture
- Can be security **analysis** of a PC or mobile application

Find your own topic and come talk to us!

You can form groups of two or three (speak to TA).



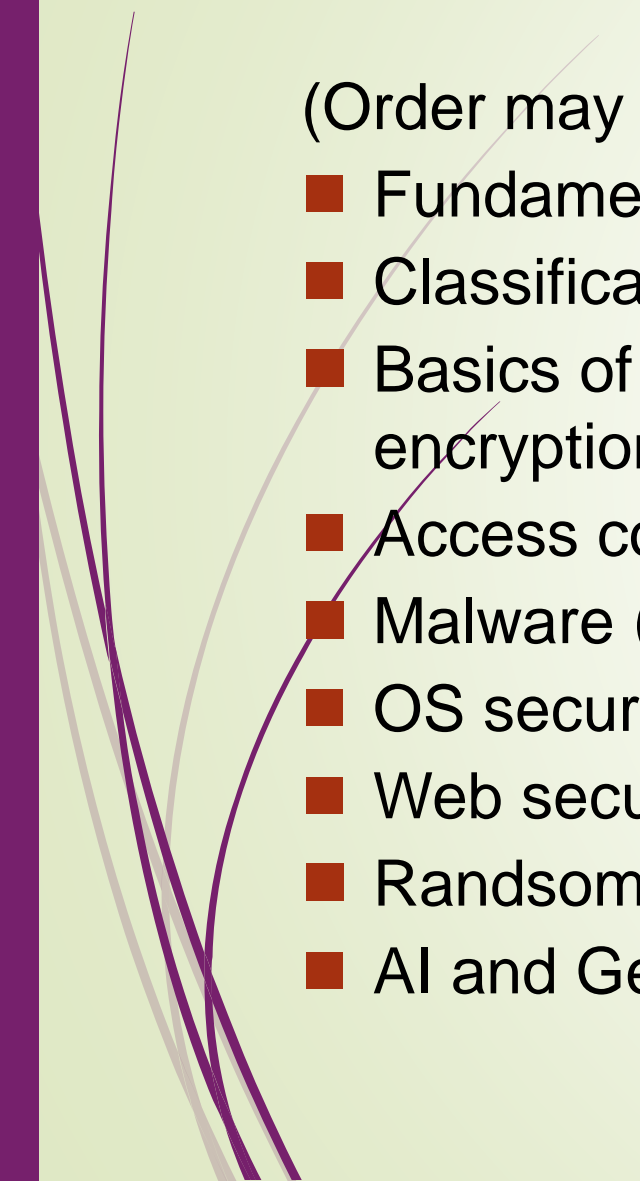
# Project

- A project topic should be selected due by the week 2.
  - A Project topic covers two topics but
    - Research + application
    - Research (Only)
  - Final report due by the end of the 13th week
- 



# Course Outline

(Order may change, topics can be added or removed.)

- Fundamental concepts and principles,
  - Classification of threats
  - Basics of cryptography, encryption-decryption, symmetric & asymmetric encryption algorithms, key distribution, electronic signatures
  - Access control, passwords, biometrics
  - Malware (virus, worm, spyware etc.)
  - OS security, Network security, IDS, IPS
  - Web security, Email security, Spam, etc.
  - Ransomware
  - AI and GenAI Security
- 



# Homeworks

The first home work:

1. Define (personally): Basic terms (data, information, knowledge, security, safety, etc.)
2. How to Protect your personal information assests, policy, evaluation



# TERM PROJECT?

For example:

- Designing a AI based Firewall



# RESOURCES

- Cole, E., Krutz, R., Conley, J.W., “Security Assessments, Testing, and Evaluation”, Network Security Bible, *Wiley Publishing Inc.*, Indianapolis, 607-612 (2005).
- Abrams, D., M., “FAA System Security Testing and Evaluation”, *Mitre Center for Advanced Aviation System Development McLean, Virginia* (2003).
- Layton, P., T., “Penetration Studies – A Technical Overview”, *SANS Institute* 2002.
- Mathew, T., “Ethical Hacking and Countermeasures EC-Council E-Business Certification Series” Copyright © by EC-Council Developer Publisher *OSB Publisher* ISBN No 0972936211.
- Klevinsky, T., J., Laliberte, S., Gupta, A., “Hack I.T.: Security Through Penetration Testing”, Publisher: *Addison Wesley First Edition* February 01, 2002 ISBN: 0-201-71956-8, 544 pages.
- Bilgi Teknolojisi— “Bilgi Güvenliği için uygulama prensibi TS ISO/IEC 17799 Standartı” Türk Standartları Enstitüsü, 2005
- Cryptography And Network Security Principles And Practices" Stallings Will, Prentice Hall, 2003.

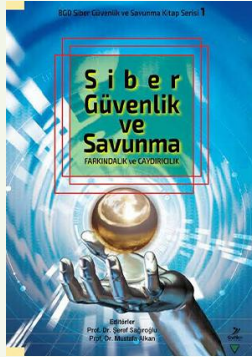
# RESOURCES

- Security Engineering, R. Anderson, Wiley, New York, 2001
- Kurumsal Bilgi Güvenliği Standartları
- Ş. Sağıroğlu, M. Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, 2006, Ankara.",
- G. Canbek, Ş. Sağıroğlu, Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Grafiker Ltd. Şti. Aralık 2006.
- Bilgi ve Bilgisayar Güvenliği Ders Notları, 2007
- D Salomon, "**Data Privacy: Encryption and Information Hiding**, 0387003118, 480 pages, Springer-Verlag New York Inc., 2003.
- K.S. Schmeih, "**Cryptography and Public Key Infrastructure on the Internet**, 047084745X, John Wiley and Sons Ltd, 2003.
- **Enterprise Information Security and Privacy**, [C. Warren Axelrod](#) (Author, Editor), **Jennifer L. Bayuk** (Editor), [Daniel Schutzer](#) (Editor), Artech House, 2009.

# RESOURCES

## ➤ Siber Güvenlik ve Savunma Kitap Serisi

➤ 1:



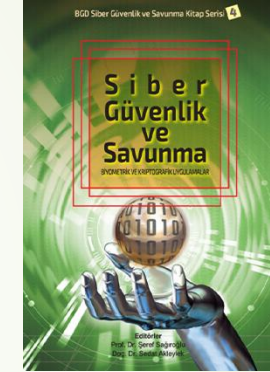
➤ 2:



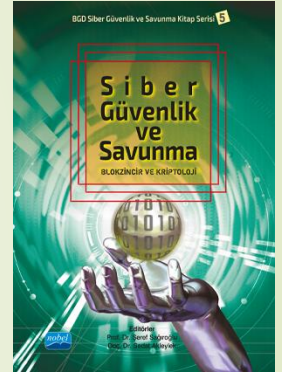
➤ 3:



➤ 4:



➤ 5:



➤ 6:

## ➤ Yapay Zeka ve Büyük Veri Kitap Serisi

➤ 1-5

➤ All Books are free and can be downloaded and disseminated free of charge.

# RESOURCES

**CIS** - The Center for Internet Security is an independent, nonprofit organization with a mission to create confidence in the connected world.

- CIS Top 20
- Hardening Templates

**NIST** - The National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.

- NIST CSF
- NIST 800 - 53



# RESOURCES

**CISA** - The Cybersecurity and Infrastructure Security Agency leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life.

- ➡ **Referential Guidance**

**OWASP** - The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.

- ➡ **OWASP Top 10**

# RESOURCES

**CSA** - Cloud Security Alliance, the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

- ➔ **White Papers and Referential Guidance**

**SANS Institute** – The SysAdmin, Audit, Network, and Security Institute offers comprehensive, intensive training designed to help anyone, from auditors to CIOs to defend systems and networks against the most dangerous threats.

# RESOURCES

**Private Tech Industry** – Microsoft, Amazon, Verizon, Google, Cisco, VMware, IBM

- ➡ Published white papers, reference architectures, comprehensive documentation, RTFM.

**Cybersecurity News Outlets** – Krebs, IT Security Guru, Security Weekly, Hacker News, Blogs

## **Certification**

- ➡ SANS, ISC<sup>2</sup>, CSA, CEH, ISACA, CompTIA





# Q&A