CS 772/872 Advanced Computer and Network Security

Course Syllabus

1. Course Information

Course Credit: 3 Credit Hours
Semester: Spring 2026
Modality: In-Person
Location & Time: As listed in the ODU Schedule of Classes

2. Instructor Information

Lead Faculty: Dr. Mohammad GhasemiGol
Email: mghasemi@odu.edu
Office Hours: By appointment (in person or virtual)

3. Course Description

This course is a research-oriented, graduate-level course, centering around basic protocols and technique, as well as advanced, state-of-the-art topics to secure computer and Internet services. Topics include: System and Software Security, Cryptography and PKI, Internet Infrastructure and Network Security, Web and Browser Security, Cloud Security, and Online Privacy.

A particular emphasis is placed on network attacks, prevention, detection, and defense techniques. Students will also explore how ML/AI techniques can enhance computer and network security. Students will analyze academic papers, prepare technical reports, and deliver presentations on emerging challenges and solutions in computer and network security.

4. Course Objectives

By the end of the course, students will be able to:

- Understand and evaluate advanced threats across system, software, and network layers.
- Analyze major classes of network attacks.
- Design and assess prevention strategies within a defense-in-depth model.
- Generate and analyze attack graphs.
- Develop and evaluate IDS techniques, including ML-based approaches.
- Apply alert management, event correlation, and SIEM concepts.
- Perform effective incident response and forensic analysis.

- Critically analyze state-of-the-art research across security domains.
- Write and present technical security research following scientific standards.

5. Course Outcomes

Students completing this course will gain:

- A deep understanding of network security attacks, detection, and defense.
- Research-level exposure to advanced security challenges and open problems.
- The ability to apply AI/ML techniques to security analytics tasks.
- Improved scientific writing and presentation skills through research papers and technical reports.

6. Course Materials

Required Textbook: None.

Recommended Resources:

- *Security Engineering*, Ross Anderson
- *Network Security Essentials*, William Stallings
- *Computer Security: Art and Science*, Matt Bishop
- NIST SP 800 series
- OWASP Top 10
- MITRE ATLAS
- Academic papers from IEEE TDSC, ACM TOPS, Computers & Security, IEEE S&P, USENIX Security, NDSS, ACM CCS, RAID, and other top journals and conferences.

7. Evaluation and Grading

This course is research-oriented, and students are expected to engage deeply with current academic work in computer and network security. The evaluation structure reflects a graduate-level research workflow, moving from topic exploration, literature review, idea development, experimentation, and final technical writing. All components will be evaluated according to detailed rubrics provided on the course site. Students are required to refer to the rubric for expectations, grading criteria, and performance standards.

7.1. Evaluation Breakdown

Component	Weight
Review Presentation (Literature Review)	25%
Research Presentation	25%
Research Paper (IEEE format)	40%
Participation & Discussions	10%
Assignments & Research Contributions (optional)	+20%

7.2. Grading Scale for CS 772

Percentage	Letter Grade
100–93	A
92–88	A-
87–84	B+
83–80	B
80–75	B-
75–70	C+
69–65	C
64–60	C-
59–55	D+
54–50	D
49–45	D-
< 45	F

7.3. Grading Scale for CS 872

Percentage	Letter Grade
100–96	A
95–93	A-
92–89	B+
88–85	B
84–80	B-
79–76	C+
75–72	C
71–68	C-
67–64	D+
63–60	D
59–55	D-

7.4. Incomplete Grades

A grade of "I" indicates assigned work yet to be completed in a given course, or absence from the final examination, and is assigned only upon instructor approval of a student request. The "I" grade may be awarded only in exceptional circumstances beyond the student's control. The "I" grade becomes an "F" if not removed by the day grades are due for the following term, based on the criteria defined in the university policy regarding Incomplete, Withdraws, and Z grades.

8. Research Process and Expectations

8.1. Topic Selection (Beginning of Semester)

During the first two weeks of the semester, each student must select a research topic related to advanced computer or network security. Topics must be:

- Relevant to course themes
- Researchable within the semester timeframe
- Approved by the instructor

Students should begin collecting recent papers (top journals and conferences encouraged) and developing an understanding of the problem space.

8.2. Review Presentation (Literature Review)

This is the first major presentation. Students must:

- Review recent research papers (more than 10 recommended)
- Summarize key contributions, methodologies, datasets, and findings
- Critically discuss limitations of existing work
- Propose possible research directions or ideas for improvement, extension, or both
- Identify gaps that their research could address

This presentation demonstrates students' ability to read, understand, and critique security research.

8.3. Research Development and Experimentation Phase (Mid–Late Semester)

After the literature review, students will select one research idea chosen based on feasibility, novelty, and instructor guidance and focus on developing it for the remainder of the semester.

Students are expected to:

- Implement prototypes, algorithms, models, or experiments
- Collect and analyze results
- Compare performance against baselines when appropriate
- Conduct iterative refinement
- Meet regularly with the instructor for guidance

8.4. Research Presentation

The second presentation showcases the student's original contribution. Students must present:

- Research motivation and problem definition
- Proposed method or idea
- Experimental design and evaluation methodology
- Results, analysis, and insights
- Discussion of limitations and possible future extensions

This simulates a conference-style research talk.

8.5. Final Research Paper (IEEE Format)

Students will submit a technical report in IEEE conference format. The paper should resemble a research publication and must include:

- Abstract
- Introduction and problem motivation
- Related work (summarized from literature review)
- Proposed method or idea
- Experimental setup
- Results and evaluation
- Discussion and limitations
- Conclusion and future work
- References

Students are encouraged to refine the paper to a publishable level.

9. Attendance Policy

Regular attendance is strongly encouraged, as in-class discussions, research feedback, and presentations are essential components of the course. If you must miss a class, please notify the instructor in advance when possible and consult Canvas for posted materials.

Students are encouraged to:

- Attend every class session
- Actively participate in discussions
- Engage respectfully with peers' ideas
- Prepare readings and research materials in advance

Quality participation includes thoughtful questions, constructive feedback, and engagement with research content.

10. Student Accountability and Academic Integrity

The Office of Student Conduct & Academic Integrity (OSCAI) oversees the administration of the student conduct system, as outlined in the Code of Student Conduct. Old Dominion University is committed to fostering an environment that is safe and secure, inclusive, and conducive to academic integrity, student engagement, and student success. The University expects students and student

organizations/groups to uphold and abide by standards included in the Code of Student Conduct. These standards are embodied within a set of core values that include personal and academic integrity, fairness, respect, community, and responsibility.

Violations of academic integrity include, but are not limited to, the following:

10.1. Cheating

Using unauthorized assistance, materials, study aids, or other information in any academic exercise. Examples include, but are not limited to:

- Using unapproved resources or assistance to complete an assignment, paper, project, quiz, or exam
- Collaborating in violation of a faculty member's instructions
- Submitting the same, or substantially the same, paper to more than one course for academic credit without first obtaining approval from the faculty

10.2. Plagiarism

Using someone else's language, ideas, or other original material without acknowledging its source in any academic exercise. Examples include, but are not limited to:

- Submitting a research paper obtained from a commercial research service, the Internet, or another student as if it were original work
- Making simple changes to borrowed materials while leaving the organization, content, or phraseology intact
- In a group project, attempting to take credit for the work of the group without participating in the work or activities of the group

10.3. Fabrication

Inventing, altering, or falsifying any data, citation, or information in any academic exercise. Examples include, but are not limited to:

- Citing a primary source that was actually obtained from a secondary source
- Inventing or altering experimental data without appropriate documentation (such as statistical outliers)

10.4. Facilitation

Helping another student commit, or attempt to commit, any Academic Integrity violation, or failing to report suspected Academic Integrity violations to a faculty member. An example of facilitation includes circulating course materials when the faculty member has not explicitly authorized their use.

10.5. Honor Pledge

By attending Old Dominion University, you have accepted the responsibility to abide by the Honor Pledge:

> I pledge to support the Honor System of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community, it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned.

11. University Email Policy

With the increasing reliance and acceptance of electronic communication, email is considered an official means for University communication. Old Dominion University provides each student an email account for the purposes of teaching and learning, research, administration, and service. It is the responsibility of every eligible student to activate MIDAS, the Monarch Identification and Authorization System, in order to obtain email access.

It is important that all students are aware of the expectations associated with email use as outlined in the Student Email Standard. The email account provided by the University is considered to be an official point of contact for correspondence. Students are expected to check their official e-mail account on a frequent and consistent basis in order to stay current with University communications.

Mail sent to the ODU email address may include notification of University-related actions, including academic, financial, and disciplinary actions. For more information about student email, please visit Student Computing.

11.1. Educational Uses of Email

University offices and instructors cannot validate that a communication coming by email is from an ODU student unless it comes from a valid ODU email address. If students send mail from non-ODU email accounts (e.g., Hotmail or Yahoo), faculty and staff are not obligated to respond and may request that official e-mail accounts be used.

12. Withdrawal

A syllabus constitutes an agreement between the student and the course instructor about course requirements. Participation in this course indicates your acceptance of its teaching focus, requirements, and policies. Please review the syllabus and the course requirements as soon as possible. If you believe that the nature of this course does not meet your interests, needs, or expectations, if you are not prepared for the amount of work involved, or if you anticipate assignment deadlines or abiding by the course policies will constitute an unacceptable hardship for you, you should drop the course by the drop/add deadline, which is listed in the ODU Schedule of Classes. For more information, please visit the Office of the University Registrar.

13. Privacy of Student Information

Old Dominion University recognizes its duty to uphold the public's trust and confidence, not only in following laws and regulations, but in following high standards of ethical behavior. Members of the Old Dominion University community are responsible for maintaining the highest ethical standards and principles of integrity. The Code of Ethics is a set of values-based statements that demonstrate the University's commitment to this goal. The Privacy of Student Information details the Family Educational Rights & Privacy Act (FERPA), along with other information regarding student privacy.

14. Disability Accommodations

In order to receive consideration for reasonable accommodations, you must contact the appropriate services office. The office will provide you with an accommodation letter. Please share this letter with your instructors and discuss the accommodations with them as early in your courses as possible. The details of disability accommodations are documented in ODU Policy #4500.

15. Discrimination and Harassment

The university is committed to equal access to programs, facilities, admission, and employment for all persons. It is the policy of the university to maintain an environment free of harassment and free of discrimination against any person because of age, race, color, ancestry, national origin, religion, creed, service in the uniformed services (as defined in state and federal law), veteran status, sex, sexual orientation, marital or family status, pregnancy, pregnancy-related conditions, physical or mental disability, gender, perceived gender, gender identity, genetic information, or political ideas. Discriminatory conduct and harassment, as well as sexual misconduct and relationship violence, violate the dignity of individuals, impede the realization of the university's educational mission, and will not be tolerated. Gender-based sexual harassment, including sexual violence, are forms of gender discrimination in that they deny or limit an individual's ability to participate in or benefit from University programs or activities. These policies shall not be construed to restrict academic freedom at the university, nor shall they be construed to restrict constitutionally protected expression. The policy is codified in University Policy #1005.

16. Copyright

All course materials students receive or to which students have online access are protected by copyright. Students may use course materials and make copies for their own use as needed; however, unauthorized distribution, sharing, or uploading of materials without the instructor's express permission is strictly prohibited.

17. Expanded Topics

Module 1: Course Overview and Foundations of Computer and Network Security

- Course overview
- CIA triad, threat models, attacker capabilities
- Vulnerabilities
- Network threat landscape overview
- Open problems and possible research topics

Module 2: Cryptography

- Symmetric and asymmetric cryptography
- TLS and secure channel protocols
- Public Key Infrastructure (PKI)
- Attacks on cryptographic protocols

Module 3: Network Attacks

- Probing and scanning
- DoS and DDoS attacks
- R2L attacks (credential guessing, remote exploitation)
- U2R attacks (privilege escalation, kernel exploitation)
- Routing and DNS attacks

Module 4: Prevention Methods

- Security architecture and layered defense models
- Firewall design and operation
- Attack graphs for modeling propagation and risk
- Vulnerability scanning and patching strategies

Module 5: Network Monitoring and Intrusion Detection Systems (IDS)

- Host-based vs. network-based IDS
- Signature-based detection vs. anomaly detection
- Dataset challenges: NSL-KDD, UNSW-NB15, CICIDS
- Encrypted traffic detection

Module 6: Alert Management, SIEM, and Security Analytics

- Log collection, normalization, aggregation pipelines
- Alert correlation, prioritization, triage
- ML for alert clustering, scoring, and noise reduction
- SIEM platforms

Module 7: Incident Response and Automated Reaction

- NIST Incident Response Lifecycle
- Evidence handling
- Automated response strategies
- Reinforcement Learning for adaptive response

Module 8: Advanced Research Topics: Web Security, Cloud Security, and Privacy

- Web and browser security (XSS, CSRF, sandboxing)
- Cloud security models, virtualization, container isolation
- Online privacy: fingerprinting and anonymization
- AI-driven attack and defense strategies

18. Course Schedule

Week	Date	Topics / Activities
1	Jan 21	Course introduction and logistics; overview of course structure and evaluation; basic security concepts including CIA triad, threat models, attacker capabilities, and security goals.
2	Jan 28	Discussion of potential research areas aligned with system, network, and AI-driven security; guidance on selecting feasible research topics.
3	Feb 4	Fundamentals of cryptography: symmetric and asymmetric encryption, hashing, and authentication; overview of common cryptographic protocols; discussion of classical and modern cryptographic attacks.
4	Feb 11	Network attack taxonomy and threat landscape; scanning and reconnaissance techniques; DoS and DDoS attacks.
5	Feb 18	Advanced network attacks; analysis of attack vectors and attacker methodologies.
6	Feb 25	Defense-in-depth security architecture; layered security models; firewall design principles; packet filtering, stateful inspection, and next-generation firewalls.

Week	Date	Topics / Activities
7	Mar 4	Attack graphs and security modeling; vulnerability correlation; risk assessment; applications of attack graphs in prevention and defense planning.
8	Mar 11	Intrusion Detection Systems fundamentals; host-based vs. network-based IDS; signature-based vs. anomaly-based detection; overview of benchmark datasets.
–	Mar 18	Spring Holiday – No Class
9	Mar 25	Student literature review presentations; discussion of gaps, limitations, and future research directions.
10	Apr 1	Alert management systems; log collection and normalization; alert correlation and prioritization; introduction to SIEM concepts.
11	Apr 8	Incident response and recovery; NIST Incident Response Lifecycle; evidence handling and forensics basics.
12	Apr 15	Applications of AI, ML, and RL in network security; intelligent firewalls; ML/AI-based IDS; automated alert management and response systems.
13	Apr 22	Advanced security topics including web and browser security, cloud security models, virtualization and container security, and online privacy challenges.
14	Apr 29	Student research presentations; presentation of original research contributions; course wrap-up and discussion of emerging research directions.