LASSONDE SCHOOL OF ENGINEERING | YORK U

Electrical Engineering and Computer Science

EECS4482 – Network Security and Forensics

Ruba Al Omari

Fall 2024

1. Important Dates

Classes Start	Classes End	Last day to drop a course without receiving a grade	Fall Study Day (No classes)	Final Exam Period
Sept. 4, 2024	Dec. 3, 2024	Nov. 8, 2024	Dec. 4, 2024	Dec. 5-20, 2024

2. Course Schedule

Type	Day	Time	Location	Cat #
Lecture	Tuesday Thursday	11:30 am – 1:00 pm	LSB 101 Keele	S88C01

3. Instructor Contact Information & Office Hours

Instructor Name	Office	Office Hour (Starting Week 2)	Email
Ruba Alomari	Lassonde 2013	Thursdays 4:15-5:15 PM	alomari@yorku.ca

Laboratory/Teaching Assistant Name	Office	Office Hour	Email

4. Course Description:

This course provides a comprehensive coverage of theoretical and practical aspects of network security and forensics. The emphasis is on the limitations and attacks against

network protocols and architectures most widely used in practice, as well as the best known detection, prevention and remediation techniques against these attacks. The course also has a strong emphasis on hands-on learning either by using already existing real-world tools or by developing new custom software.
Familiarity with the TCP/IP protocol suite and basic computer networking concepts is required.

Topics covered include:

1) Analysis of weaknesses and attacks against the most common Internet protocols such as IPv4, IPv6, TCP, ICMP, ARP, DHCP, and DNS.
2) Secure protocols including IPSec, TLS, and DNSSEC.
3) Network scanning and OS fingerprinting.
4) Packet inspection and log analysis.
5) Developing software for packet and log manipulation.
6) Virtual private networks (VPNs), and tunneling.
7) Network design, firewalls, packet filters, proxies, NAT, ingress and egress filtering.
8) Intrusion detection systems.
9) Network forensics investigation methodology and tools.
10) Tentative Topics if time permits: Wireless security, Cloud security.

Prerequisites: EECS3213-Communication Networks or EECS3214-Computer Network Protocols and Applications, and EECS3482-Introduction to Computer Security.

5. Expected Learning Outcomes

By the end of the course, the students are expected to be able to:

1) Demonstrate proficient knowledge of the main security problems/deficiencies found in the most common Internet protocols and network architectures.
2) Qualitatively discuss the key features, as well as the main pros and cons of using the secure versions of the most common Internet protocols (IPsec, TLS, DNSSEC, ...)
3) Evaluate the effectiveness (or lack of adequate) security controls in a given network.
4) Propose the best approaches to hardening a given network – either by using proper secure network protocols, by modifying network configuration, or by utilizing specialized network-security (software or hardware) appliances.
5) Build a custom software to solve a particular network security problem.
6) Analyze a packet trace or a network log for signs/evidence of security compromise.

6. Required Textbook/Readings

- Internet Security: A Hands-on Approach (3rd ed., 2022), by Wenliang Du, ISBN: 978-17330039-6-4. (Available from York Library in hard copy)

Additional readings may be assigned or recommended during the course.

7. Schedule

Week	Week Of	Tue	Thu	Topics	Readings*
1	Sept. 2	–	Lecture	**Network Security Basics** Introduction – Network Primer Environment Setup Tools of the Trade Sniffing and Spoofing Scanning and Enumeration	Ch. 1 & 4
2	Sept. 9	Lecture	Lecture		
3	Sept. 16	Lecture	Lecture		
4	Sept. 23	Lecture	Lecture	**Attacks on Protocols** MAC Layer – ARP & Attacks Network Layer – IP & Attacks Transport Layer – UDP & Attacks TCP Protocol & Attacks	Ch. 2, 3, 5, & 6
5	Sept. 30	Lecture	Lecture		
6	Oct. 7	Lecture	Lecture		
	Oct. 14-Oct. 18	Reading Week – No Classes			
7	Oct. 21	**Midterm**	Lecture	DNS & Attacks, DNSSEC BGP and Attacks	Ch. 10, 11 & 12
8	Oct. 28	Lecture	Lecture		
9	Nov. 4	Lecture	Lecture	**Defense Mechanisms** Virtual Private Network Transport Layer Security IDPSs & Firewalls	Ch. 7, 8 & 19
10	Nov. 11	Lecture	Lecture		
11	Nov. 18	Lecture	Lecture		
12	Nov. 25	Lecture	Lecture	Hack Something Project Presentation	
13	Dec. 2	Lecture	–	Hack Something Project Presentation	
	Dec. 4	Fall Study Day – No Classes			

* All chapters refer to the Internet Security textbook.

8. Assessment

- Assessment is as follows:
    - **25% Labs – 5 Labs @ 5% each.**
      Check eClass for due dates.

- **15% Hack Something Group Project.**
  Check eClass for due dates.

- **20% Midterm Test**
  Date specified in the schedule section.

- **40% Final Exam**
  Scheduled by the registrar's office.

- The default and only acceptable way of submission for assessments in this course is through eClass, unless otherwise specified. Email submissions are void for all assessments.
- Conversion of the overall numeric mark to a letter grade:

F	E	D	D+	C	C+	B	B+	A	A+
<40	>= 40	>= 50	>= 55	>= 60	>= 65	>= 70	>= 75	>= 80	>= 90

For a full description of York grading system see the York University Undergraduate Calendar - https://calendars.students.yorku.ca/2022-2023/grades-and-grading-schemes

Student Expectations & Course-Specific Policies

9. Missed Assessments

Students who miss the due date for a lab, can still submit within 48 hours with a 25% late submission penalty. Students who fail to submit within 48 hours, must submit a request for consideration with supporting documentation to the instructor in writing within 3 days of the missed lab (late submission penalty still applies).

Students who miss the midterm must submit a request for consideration with supporting documentation to the instructor in writing within 5 days of the missed midterm.

For missed final exams, students must submit a petition through the department to write a deferred exam.

If a student misses coursework and does not follow the procedures listed above, the student will receive zero marks for the missed coursework.

10. Grade Appeals

If you believe there is an error, follow the instructions in the test results announcement on submitting a reappraisal request online. It is essential that you present logical arguments as to why the work should be re-marked; otherwise, it will not. Note that the entire work will be

re-marked, and your mark may be increased or decreased, or it may stay unchanged. Note also that the deadline for grade appeal is **5 business days** after the marks are posted. No grade appeal request will be considered after that deadline.

11. Asking Questions

1. Use the course forum to ask any course-related questions. This is the best and fastest way to get answers. You are also encouraged to answer posted questions as this is a great way to learn. To use the forum, you must adhere to the **forum protocol**:

    - Do not ask a question that has already been asked or whose answer has already been posted. To that end, use the search facility to look for keywords related to your question.
    - Be clear and specific. This applies to the post title as well as to its body. For example, "Please Help" is not a good title, and "My code is not working" is not useful --instead, provide the exception message and the code.
    - Do not mix topics. If while answering a question, you think of a different question, then post it in a separate topic.
    - Be professional in terms of language and tone.

2. For questions related to private matters requiring confidentiality send me an email (alomari@yorku.ca). The **email protocol** is as follows:

    - Put "EECS 4482/X" in the subject line where X is your PPY (Passport York) username.
    - Include your full name in the message body. Do not include your York ID.
    - Email messages not meeting these guidelines, or not requiring confidentiality, will **not** be answered.

12. Recording

Students may not record any portion of a lecture, class discussion, or other learning activity without the prior knowledge and written consent of the instructor.

13. Silent Policy

A silent policy takes effect 24 hours before an assignment is due. This means that no questions about any assignment/term test/group project will be answered whether it is asked on the bulletin board, by email, through Canvas messages, or in person.

14. Academic Honesty Policy

Students are expected to act with integrity. For assignments, projects, and activities, students may discuss the questions with others, may ask questions on forums, and may look for ideas online, but once they understand the approach, they must compose and

submit their own answers. For tests and exams, students may not communicate with anyone by any means. By submitting any assessment, you acknowledge that you are aware of these rules and that we may enforce them in a variety of ways; e.g., monitor network traffic, use video cameras, mine for patterns, administer multiple versions, etc. Violators (whether committing or aiding) will be charged with academic dishonesty whose penalty may reach expulsion from the University.

Students are expected to read and understand the **Senate Policy on Academic Honesty** available at https://www.yorku.ca/secretariat/policies/policies/academic-honesty-senate-policy-on/

and **Academic Conduct Policy and Procedures** available at https://www.yorku.ca/secretariat/policies/policies/academic-conduct-policy-and-procedures/

Note that if the links are not active, you can google "Senate Policy on Academic Honesty York University" and "Academic Conduct Policy and Procedures" to find an alternate link.

15. Access/Disability

York University is committed to principles of respect, inclusion, and equality of all persons with disabilities across campus. The University provides services for students with disabilities (including physical, medical, learning, and psychiatric disabilities) needing accommodation related to teaching and evaluation methods/materials. These services are made available to students in all Faculties and programs at York University. Students in need of these services are asked to register with disability services as early as possible to ensure that appropriate academic accommodation can be provided with advance notice. You are encouraged to schedule a time early in the term to meet with each professor to discuss your accommodation needs. Please note that registering with disabilities services and discussing your needs with your professors is necessary to avoid any impediment to receiving the necessary academic accommodations to meet your needs.

To learn more about academic accommodation for students with disabilities policy visit: https://www.yorku.ca/secretariat/policies/policies/academic-accommodation-for-students-with-disabilities-policy/ and Counseling and Disability Services available at https://accessibility.students.yorku.ca/

16. York University's Support and Policy on Sexual Violence

The Centre for Sexual Violence Response, Support, and Education is the University office with the primary responsibility to assist community members affected by sexual violence. The Centre coordinates support and resources for those who have experienced sexual violence, receives disclosures and complaints, facilitates safety planning, and assists survivors through the complaint process.

To learn more about York University Policy on Sexual Violence, and existing Supports and Services for Students, visit https://www.yorku.ca/secretariat/policies/policies/sexual-violence-policy-on/

17. Copyright

Course materials are designed for use only in the course. Copying this material for distribution (e.g., uploading material to a third-party website) may lead to a charge of misconduct under York's Code of Student Rights and Responsibilities and the Senate Policy on Academic Honesty and/or legal consequences if copyright law has been violated http://www.copyright.info.yorku.ca

18. Campus Policies

- Academic Integrity: http://www.yorku.ca/academicintegrity
- Student Code of Rights and Responsibilities: https://calendars.students.yorku.ca/2022-2023/code-of-student-rights-and-responsibilities
- Accommodations for Students with Disabilities: https://calendars.students.yorku.ca/2022-2023/academic-accommodation-for-students-with-disabilities
- Academic Policies and Regulations: https://calendars.students.yorku.ca/2022-2023/policies-and-regulations
- Ethics review process for research involving human participants: https://www.yorku.ca/research/research-ethics /
- Student conduct standards: https://calendars.students.yorku.ca/2022-2023/student-conduct-and-responsibilities
- Religious Accommodation: https://calendars.students.yorku.ca/2022-2023/religious-accommodation

19. Computer Session Monitoring During Labtest:

Labtest will be used when writing tests and exams in this course. Please ensure to read the disclaimer available at this link prior to writing your test: https://www.eecs.yorku.ca/teaching/docs/disclaimer-labtest-monitoring.pdf

Note that this monitoring is only being done during in-lab labtest, and only on department owned equipment (never on student personal equipment such as their desktops or laptops).

Students can email their concerns to: Tech support (tech@eecs.yorku.ca), undergraduate program director, Gene Cheung (genec@yorku.ca), or Lassonde's Associate Dean of Students, Mitchell Burnie (mitch.burnie@lassonde.yorku.ca)

DISCLAIMER: Computer Session Monitoring during Labtests

This disclaimer serves to inform all students participating in in-lab tests (labtests) that electronic proctoring may occur, and their computer session may be monitored by their instructor. By accessing and utilizing labtest, you acknowledge and accept the following terms and conditions: **1. Purpose of electronic proctoring:** The monitoring of computer sessions during labtest is carried out for the purpose of maintaining academic integrity, ensuring fairness in assessment, enabling electronic communication between students and instructors, and promoting a conducive learning environment.

2. Academic Integrity: Clear instructions and access to approved materials for the test are provided. The monitoring process aims to deter and detect any unauthorized activities that may compromise the integrity of the examination or violate Senate policy.

3. Remote Troubleshooting: In the event of technical difficulties or disruptions encountered during the labtest, authorized personnel may access and monitor your computer session to provide remote troubleshooting support, address technical issues promptly, and minimize any potential interruptions to your labtest experience.

4. Maintenance and Security: Monitoring may be conducted for the purposes of system maintenance, ensuring the security of the testing platform, and identifying and mitigating any potential vulnerabilities or threats.

5. Confidentiality and Data Protection: All monitoring activities will be carried out in accordance with applicable privacy laws and regulations.

6. Legal Compliance: By accessing and participating in computer-based tests, you agree to comply with all relevant laws, regulations, institutional policies, and codes of conduct. Failure to comply may result in disciplinary action, including but not limited to the nullification of test scores, academic penalties, or other appropriate consequences as determined by the Lassonde School of Engineering.

7. Liability Disclaimer: The educational institution and its authorized personnel shall not be held responsible for any technical issues, disruptions, data loss, or any other consequences arising from the monitoring activities conducted during the test.

8. Acceptance: By proceeding to use labtest, you acknowledge that you have read, understood, and agreed to the terms and conditions outlined in this disclaimer. If you have any concerns or questions regarding the monitoring process, please seek clarification from: tech@eecs.yorku.ca .