CSEC-759: Graduate Seminar in Computing Security Course Syllabus

NOTE: The information presented in this syllabus is subject to expansion, change, or modification during the semester.

Course Description

In this course, students will gain in-depth knowledge on analysis approaches that reveal malware behavior on infected machines and techniques used by malware to evade analysis. Students will explore current research in the malware domain and learn to use tools such as Cuckoo Sandbox, Volatility, and Google Rapid Response.

As a **research seminar**, this course emphasizes exploring and understanding the **current state-of-the-art in the malware domain**. Students will critically examine recent advancements, research papers, and emerging trends. Through discussions, paper reviews, and hands-on projects, students will develop the skills necessary to contribute to ongoing research conversations in this area.

This research-oriented course encourages students to engage with academic literature and open-source tools. While studying source code is not required, it is highly recommended.

Course Learning Outcomes

Learning Outcome	Assessment Method(s)
Use malware analysis tools for dynamic, memory, and enterprise-level analysis	Hands-on Activity, Final Project
Critically analyze current malware research literature.	Paper Review Assignments, Class Discussions
Identify malware evasion techniques and recommend countermeasures.	Paper Review Assignments, Hands-on Activities, Final Project
Evaluate traditional malware detection methods.	Class Discussions, Paper Review Assignments
Distinguish between malware types (e.g., viruses, worms, rootkits).	Foundational Knowledge Applied Across all Activities
Discuss ethical considerations in malware analysis.	Class Discussions

Synthesize insights from state-of-the-art research papers and propose innovative approaches.	Paper Review Assignments, Final Project
Develop and present research findings related to malware analysis.	Final Project

Prerequisites

None

Course Materials

RIT MyCourses will be used to access course content, submit assessments (e.g., assignments), complete quizzes, and view grades.

Required Materials

- **Readings:** Weekly assigned articles available via myCourses or RIT Library.
- **Software Tools:** Open-source tools such as Cuckoo Sandbox, Volatility, and Google Rapid Response.
- **Optional Textbooks:**
  - *Practical Malware Analysis* (Sikorski & Honig)
  - *The Art of Memory Forensics* (Ligh et al.)
  - *The Rootkit Arsenal* (Blunden)

Expectations

This is a 3-credit semester course. You should plan to spend several hours each week outside of the classroom to complete the work required for this course, in addition to the time you attend and participate in class.

Important RIT Deadlines

For term dates, including add/drop and withdrawal deadlines refer to the RIT Calendar.
Use the arrows at the top and bottom of the page to review additional syllabus information.

Instructor Information

Instructor: Nate Mathews

- Office Location:
- Email:
- Office Hours: Days/Times: Thursdays 11-12 EST, or schedule via email

I will answer emails and messages within 24 hours between Monday and Friday. Responses to emails and messages received on Saturdays, Sundays, breaks, or holidays may be delayed. I will respond to those emails and messages within 48 hours of the next academic day.

Expectations

All course content, topics, concepts, skills, techniques and tools within this course are for educational and research purposes only. Your use of them must be legal, ethical, moral, responsible, and professional. Contact your instructor with any questions and/or concerns.

Students are expected to adhere to the following. Failure to adhere to these will result in failing the course and being considered for expulsion from RIT. Degree revocation may also be considered. If you do not agree with these expectations or cannot or will not adhere to them, you should drop the course during the add/drop period or withdraw from the course.

- Act and be legal, ethical, moral, responsible, and professional.
- Do not break any laws.
- Do not access any protected (e.g., password protected, etc.) systems or material for which you do not have explicit written permission.
- Only use the course content, topics, concepts, skills, techniques and tools and your knowledge, skills, and abilities for good.
- Do not use the course content, topics, concepts, skills, techniques, and tools or your knowledge, skills, and abilities for any illegal, immoral, unethical, and/or malicious activity.
- Ask the instructor any questions and discuss with the instructor any concerns prior to taking any action.

Warnings

Some course content may include additional acceptable and unacceptable actions, uses, and/or guidelines. The instructor is not a lawyer. No legal advice is provided within this course. Seek legal advice from your legal counsel.

Liability Release

The instructor assumes no liability and will not be held responsible or liable for your actions with the course content, topics, concepts, skills, techniques and tools or your use of your knowledge, skills, and abilities. In addition, the instructor assumes no liability or responsibility for errors or omissions and no liability for damages related to your use of the course content, topics, concepts, skills, techniques and tools. Therefore, the instructor is released from all liability.

Course Content & Schedule

Refer to the myCourses Content and Calendar tabs for details on availability and due dates. All times listed in the course are US Eastern time, unless otherwise noted.

Module	Content Released	Readings Assigned	Discussions Due	Assignments Due
Getting Started & Syllabus	N/A	Syllabus/Policies, Graded Activity Guidelines, Schedule	Introduce Yourself (ungraded)	Quiz: Student Identity Verification Checklist (ungraded)
Module 1: Malware Overview and Machine Learning	Week 2	Rossow et al., Ye et al., Biggio	False Positives vs. False Negatives, High Risk/High Reward (*Beginning of Week 4)*	M1PR1, M1PR2, M1PR3 (*Beginning of Week 4*)
Module 2: Static Analysis	Week 4	Aghakhani et al., Raff et al., Lucas et al.	Signature-based Detection, ML Model Interpretability (*Beginning of Week 6*)	M2PR1 (*Beginning of Week 6*)
Module 3: Dynamic Analysis	Week 6	Miramirkhani et al., Avllazagaj et al., Zhang et al.	Dynamic Analysis Applications, Adversarial ML (*Beginning of Week 8*)	M3PR1 (*Beginning of Week 8)*

Module 4: Cuckoo Sandbox	Week 8	Kharraz et al.	No Discussion	M4PR1, Cuckoo Sandbox Report (*Beginning of Week 10*)
Module 5: Memory Analysis Using Volatility	Week 10	Musavi et al.	Challenges of Memory Forensics (*Beginning of Week 12*)	M5PR1, Volatility Report (*Beginning of Week 12*)
Module 6: Enterprise-Level Investigations	Week 12	Yen et al.	Opportunities and Challenges of GRR *(Beginning of Week 14)*	M6PR1, Google Rapid Response Report *(Beginning of Week 14)*
Module 7: Final Project	Week 8	No readings assigned	No Discussion	Proposal (*Beginning of Week 10*), Update (*Beginning of Week 12*), Final Submission (*Last week of course*)

Grading

Your overall evaluation is based on the following components. Note that all graded items have associated rubrics, which are visible on the individual graded items and in the Guideline document for that graded item.

Component	Weight
Discussions (initial post and replies)	15% *(8 items total, 1.875% each)*
Paper Review Assignments	30% *(8 items total, three items worth ~1.7%; five items worth ~5.0%)*
Hands-on Activity and Report Assignments	25% *(3 items total, 8.334% each)*

Final Project	30% (5% for the proposal, 5% for the update, 20% for the final project)
Total	**100%**

Late Work Policy

Due dates for all graded items are provided on the Course Schedule. **For every day a graded item submission is past the deadline, a 5% deduction will be applied** to the overall grade allotted to that item. In other words, if a graded item is submitted within the third day after the deadline, it will be eligible for a maximum of 85% of the points allotted to that item. Graded items submitted seven days or more after the deadline will not be accepted. Discussion post assignments are exempt from this policy and posts must be submitted by the deadline to allow sufficient time for other students to reply.

If you can foresee problems that prevent you from submitting on time, alert the instructors to the issue ASAP, and at least 24 hours before the deadline. Exceptions will be made for emergencies. Work with the instructor on a new deadline.

Emailed Submissions

Submissions must be submitted to myCourses by the due date. Submissions via email or any other means to the instructors will not be accepted.

Use of Artificial Intelligence (AI)

Students are allowed to use AI tools, including large language models (LLMs), for drafting reports, aiding technical tasks, and supporting their learning process. However:

- The **final submission must reflect the student's own critical thinking, understanding, and effort**.
- AI-generated content must be **significantly edited and revised** by the student.
- Simply submitting AI-generated content with minimal changes is **unacceptable** and will result in poor marks.
- Students must **take ownership of the ideas and content** presented in their submissions.
- If AI tools are used in report writing or online discussions, students are expected to **disclose their use and describe how the tools contributed** to the final submission.

Failure to follow this policy may result in grade penalties or further academic integrity review.

Academic Integrity

As an institution of higher learning, RIT expects students to behave honestly and ethically at all times, especially when submitting work for evaluation in conjunction with any course or degree requirement. RIT requires all students to become familiar with the RIT Honor Code and with RIT's Academic Integrity Policy.

Academic Adjustments

RIT is committed to providing academic adjustments to students with disabilities. If you would like to request academic adjustments such as testing modifications due to a disability, please contact the Disability Services Office. Contact information for the DSO and information about how to request adjustments can be found at the Disability Services Office. After you receive academic adjustment approval, it is imperative that you contact me as early as possible so that we can work out whatever arrangement is necessary.

Title IX

Title IX violations are taken very seriously at RIT. RIT is committed to investigate complaints of sexual discrimination, sexual harassment, sexual assault and other sexual misconduct, and to ensure that appropriate action is taken to stop the behavior, prevent its recurrence and remedy its effects. Additional information and policies are available at:

https://www.rit.edu/fa/compliance/title-ix

https://www.rit.edu /fa/compliance/title-ix-policies-and-resources.

RIT is committed to providing a safe learning environment, free of harassment and discrimination as articulated in our university policies located on our governance website. RIT's policies require faculty to share information about incidents of gender-based discrimination and harassment with RIT's Title IX coordinator or deputy coordinators when incidents are stated to them directly. The information you provide to a non-confidential resource which includes faculty will be relayed only as necessary for the Title IX Coordinator to investigate and/or seek resolution. Even RIT Offices and employees who cannot guarantee confidentiality will maintain your privacy to the greatest extent possible.

If an individual discloses information during a public awareness event, a protest, during a class project, or advocacy event, RIT is not obligated to investigate based on this public disclosure. RIT may however use this information to further educate faculty, staff, and students about prevention efforts and available resources.

If you would like to report an incident of gender-based discrimination or harassment directly, you may do so by using the methods outlined in RIT's Sexual Harassment, Discrimination, and Sexual Misconduct Reporting policy.

If you have a concern related to gender-based discrimination and/or harassment and prefer to have a confidential discussion, assistance is available from any of RIT's confidential resources (listed below).

RIT Counseling and Psychological Services: 585-475-2261 (V), 585-475-6897 (TTY)
www.rit.edu/counseling

RIT Student Health Center: 585-475-2255 (V) www.rit.edu/studentaffairs/studenthealth

RIT Ombuds Office: 585-475-7357; 585-475-6424; 585-286-4677 (VP)
www.rit.edu/ombuds/contact-us

NTID Counseling and Academic Advising: 585-475-6400
www.rit.edu/ntid/caas

Center for Religious Life: 585-475-2137 www.rit.edu/studentaffairs/religion

Starfish

This course uses the RIT Starfish communication tool in order to promote student success. If I am concerned about a student's academic performance, I may issue an academic alert, which will notify the student and the student's advisors. If you receive an academic alert from Starfish for this course, please communicate with me, your advisor, or other appropriate contact as soon as possible to discuss the issue, its potential impact on your success in this course, and resources to assist you.

RIT Code of Conduct for Computer Use

The RIT Code of Conduct for Computer Use guides the use of computer and network resources at RIT. This is a summary of the RIT Code of Conduct. The full text is available here. The computing, network and information resources of the Rochester Institute of Technology are intended to support the mission of teaching, scholarly activity and service for the Institute's students, faculty, and staff. Appropriate use of the computer and networking facilities by members of RIT's academic community should always reflect academic honesty and good judgment in the utilization of shared resources and observe the ethical and legal guidelines of our society.

Sharing Protected Information on the Internet

When sharing copyrighted content on the Internet with your classmates, please make sure that you link to a legal source. Repeated access to illegal sources may cause you or your

classmates to receive warnings through the Copyright Alert System, as well as possible downgrades in Internet service and possible disabling of your RIT account. View more about the RIT Copyright Infringement policy.

Use of Copyrighted Material

Certain materials used in this course are protected by copyright and may not be copied or distributed by students. You can find more information at https://www.rit.edu/academicaffairs/policiesmanual/c032.

Students may not copy, publish, distribute, display, modify or create derivative works of the course materials in any medium for any purpose. Additionally, students may not sell, rent, lease, trade, or otherwise transfer the course materials.

Emergencies

In the event of a University-wide emergency, course requirements, classes, deadlines and grading schemes are subject to changes that may include alternative delivery methods, alternative methods of interaction with the instructor, class materials, and/or classmates, a revised attendance policy, a revised semester calendar, and/or a revised grading scheme. Should the campus be impacted by weather or other issues, emergency notifications should be available on a banner at the main RIT website (https://www.rit.edu) and may also be posted in other official communications.

Student Support Availability

Please feel free to reach out about any difficulty you may be having that may impact your performance in this course as soon as it occurs. In addition to your academic advisor, we strongly encourage you to contact the many other support services on campus that stand ready to assist you. These include the Academic Success Center, College Restoration Program, Disability Services, English Language Center, Higher Education Opportunity Program, Spectrum Support program, RIT Ombuds, and TRiO Support Services. Students can find out about specific services and programs at www.rit.edu/studentaffairs.

Communication

RIT email is the official communication mechanism. Email will be used to make official announcements. Students are to use email for notification of class absence, grades discussion, and requests. Students may also use email to discuss and ask questions about course topics and assignments. All academic-related communications must be sent from students' RIT email addresses.