SYLLABUS: CYBER501x Cybersecurity Fundamentals

Course description

In this graduate level introduction to the field of computing security, you will receive an extensive overview of the various branches of computing security. You will learn cybersecurity concepts, issues, and tools that are critical in solving problems in the computing security domain.

You will have opportunities to learn essential techniques in protecting systems and network infrastructures, analyzing and monitoring potential threats and attacks, devising and implementing security solutions for organizations large or small.

This offering is part of the RITx MicroMasters in Cybersecurity that prepares students to enter and advance in the field of computing security.

You will learn:

- Network and system administration fundamentals
- Information assurance fundamentals such as confidentiality, integrity and availability, etc.
- Basic cryptography concepts

Prerequisites

There are no required courses to complete before this course. However, this course is intended for those who have completed a Bachelor's degree.

This course is part of the RITx MicroMasters in Cybersecurity. The other courses in this series are:

- CYBER502x: Computer Forensics
- CYBER503x: Cybersecurity Risk Management
- CYBER504x: Network Security
- CYBER525x: Cybersecurity Capstone

Course staff

Jonathan S. Weissman
Senior Lecturer, Computing Security
Rochester Institute of Technology

Grading and certification

If you are planning to earn a verified certificate for this course, you must complete the graded quiz at the end of each week. You only have one attempt for each quiz question, so review each question carefully before saving your answer. Verified students who complete the quizzes with a cumulative 80% or higher average will earn a verified certificate from edX, signifying successful completion of the course.

There is no weekly deadline for each unit's quiz—as long as you complete all the quizzes by the course end date you will be eligible for the certificate.

Students who successfully earn a Verified Certificate in all four courses and pass the capstone will receive a MicroMasters Credential. Learners who successfully earn the MicroMasters Credential are eligible to apply to RIT's B. Thomas Golisano College of Computing and Information Sciences for graduate credential options. You can learn more about this on the Cybersecurity MicroMasters program page.

You can choose to upgrade to a verified certificate up to February 13, 2018.

Workload

To successfully complete this course, you should plan to devote 6 to 8 hours per week to the course. You will spend that time:

- Watching videos
- Reading text resources
- Taking quizzes and tests
- Completing activities

Course materials & activities

During this course, you'll draw on some outside resources, especially the TCP/IP Guide, which is an excellent source of information about networking. You'll also have a chance to observe some of the things you'll learn about on your own system.

The course consists of these units:

- Unit 0: Getting Started
- Unit 1: Computing Security Concepts and Problems 1
- Unit 2: Computing Security Concepts and Problems 2

- Unit 3: Cryptography
- Unit 4: Networking 1
- Unit 5: Networking 2
- Unit 6: Systems Administration
- Unit 7: Detection and Prevention
- Unit 8: Malware and Forensics
- Conclusion

Course components

To facilitate navigation within each unit, course materials and activities are presented with the following headings:

To help facilitate navigation within each unit, the course materials and activities are presented with the following headings:

ABOUT THIS VIDEO

Provides an introduction and summary of the topics covered in each video lecture.

CHECK YOUR UNDERSTANDING (UNGRADED QUIZ)

Ungraded questions based on the content of each video lecture.

DISCUSSIONS

Discussions are posted in their own topics in each unit and are opportunities to share your ideas and experiences, and work with other students in the course. These are not required for a grade, but we strongly encourage you to participate as much as possible.

ACTIVITIES

There are *optional, ungraded* activities that will let you see or apply some of the principles that you'll learn about.

Students who complete the Verified track of this MicroMasters will be able to participate in hands-on computer-based lab activities in the CYBER525x Capstone.

RESOURCES

Links to articles, websites, and other resources that can deepen your learning and understanding of cybersecurity. *Resources that contain information needed to complete weekly quizzes are clearly indicated.*

GRADED QUIZ

Graded quizzes at the end of each unit that are required for verified certificates. These quizzes are open to all students.

Participating in Discussions

Each unit contains a Discussion that we encourage you to participate in. Discussions are posted in their own topics and are also accessible by clicking "Discussion" on the edX toolbar. It's perfectly fine to use the discussion questions as departure points for other conversations with your classmates. Course staff occasionally monitors posts; however, because we expect a large number of students and limited resources, we may not be able to answer all questions. We appreciate your understanding.

In addition to participating in the course discussions, you can also use the Questions About this Course Forum to talk about other topics with your classmates.

Getting Help

If you have a question about content-related or technical issues that you'd like course staff to address, please add ***[Staff]*** at the beginning of your post. Please check to see if someone else has already asked your question before creating a new post.

You can access any forum by clicking "Discussion" on the toolbar at the top of your screen.

To see previous posts in any forum, click on the "Show All Discussions" tab at the left of the "Discussions" screen, and choose the appropriate category.

For more detailed instructions on how to use edX course discussions, please refer to the edX Learner's Guide under Participating in Course Discussions

Remember, your contributions must follow the **Discussion Code of Conduct** below.

Word clouds and surveys

These activities give you a chance to add your thoughts to the course environment. These are ungraded.

Academic policy

You must behave with academic honesty and respect your fellow students. Please abide by the edX Terms of Service & Honor Code.

Discussion Code Of Conduct

We are committed to providing a friendly, safe, and welcoming environment for all students. This code of conduct outlines our expectations for discussion behavior, as well as the consequences for unacceptable behavior.

- Be respectful
- Please respect your fellow students. Insulting or abusive words will not be tolerated and will be removed.
- Be constructive
- A learning community is about learning with and through engagement with one another.
- Be culturally aware

This is a global forum with participants from many different cultures and backgrounds. Be sensitive when discussing race, religion, gender, sexual orientation, or controversial topics, since others may be more sensitive about them than you are.

Post appropriately

Content that violates the edX Terms of Service & Honor Code is not permitted. You may not post inappropriate (e.g. pornographic) or copyrighted content, advertise or promote outside products or organizations, or spam the forums with repeat content.

Consequences of Unacceptable Behavior

Unacceptable behavior will not be tolerated. Anyone asked to stop unacceptable behavior is expected to comply immediately.

If a participant engages in unacceptable behavior, the course staff may take any action they deem appropriate, up to and including expulsion from the course.

Please help us create a healthy learning environment by respecting these standards. We do not expect to see many of these issues because we trust students like you to keep our forum communities strong and healthy.