MASTER SYLLABUS

CSCI-620: Operating System Security

Course Details

Semester:	Spring 2024
Course Code:	CSCI-620-VA4 (3010)
Course Name:	Operating System Security
Course Prerequisites:	CSCI 370 Intro. To Computer Networks, ITEC 385 Intro to Comp & Network Sec. or equivalents.
Course Co-requisites:	None
Credits Hours:	Three (3) credit hours
Classroom:	Broadway Tech Center Vancouver, 2985 Virtual Way, Rm. 1812
Class Timing:	(45 contact hours)

Instructor Details

Professor:	Samuel Rostam
Office Location:	In-Person Class
Office Hours:	9:00-9:30 After class Or by appointment – Via ZOOM
Email:	srostam@nyit.edu
Course website:	Canvas: https://nyit.instructure.com/courses/27270

Catalog Course Description

In this course students are introduced to advanced concepts in operating systems with emphasis on security. Students will study contemporary operating systems including Linux and Windows.

Topics include the application of policies for security administration, mandatory vs. discretionary access control, Information Flow Models, file system security, audit and logging, cryptographic enabled applications, and operating system integrity verification techniques.

Course-Level Learning Outcomes[1]

1. Differentiate the design of a Secure Operating System from a non-secure one, and compare and contrast threats to a Secure Operating System
2. Evaluate Access Control techniques such as Protection Systems and Mandatory Protection Systems
3. Critique Security in Ordinary Operating Systems such as Unix and Windows
4. Compare and contrast Techniques to Secure Commercial Operating Systems
5. Design steps to mitigate common OS security attacks
6. Assess operating systems' support for crypto and cipher
7. Communicate effectively via written and oral means
8. Function effectively in a team

Teaching and Learning Methodologies

The School of Engineering and Computing Sciences' teaching and learning strategy is informed by the school's stakeholders, including the school advisory board, individual program advisory boards, faculty, and employers. The Teaching and Learning Methodologies are further informed by institutional indirect assessment results, periodically collected and reviewed by the Office of Planning and Assessment and the school's faculty. A component of all courses, as a part of the teaching and learning strategies, is to maintain academic rigor and to be intellectually challenging.

In this course four (4) prioritized teaching and learning strategies focus on:

---

[1] Bloom's taxonomy of cognitive learning, originated by Benjamin Bloom and collaborators in the 1950's, describes several categories of cognitive learning. This taxonomy was revised in 2001 by Anderson and Krathwohl to change the category names from nouns to verbs, and to switch the Evaluation and Synthesis levels in the hierarchy. The course level learning outcomes of courses within SoECS are informed by this revised model. Please see: A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, http://www.celt.iastate.edu/teaching/RevisedBlooms1.html?utm_source=rss&utm_medium=rss&utm_campaign=a-model-of-learning-objectives

a) Teamwork/Collaborative Work
b) Solving Problems
c) Case-based Learning
d) Integrating International/Global Perspectives

All faculty members that instruct this course should consider how to execute the course to emphasize these key components of the strategies considered. Following a review of learning outcomes, faculty members consider how re-orientation of teaching and learning strategies might result in strengthening these outcomes, and adjustments are made, accordingly.

The classes will also be taught using an active and collaborative learning approach. This approach is student centered not instructor centered. The teaching approach will be multi-method. As the subjects are highly dynamic in nature, there will be some degree of experimentation. The key dimension, however, will be interaction, both among students, and between the instructors and students, utilizing case discussions and presentations of both these and completed projects.

A number of online resources, such as tutorials, video links and simulations complement the traditional learning resources. Also individual faculty may choose to employ online learning management systems (LMS) (NYIT has an institutional license for Blackboard™) to complement the classroom based learning methodologies. LMSs can be used to foster moderated discussions, as well as provide a forum for team-based assignments and projects.

Resources

Textbook(s)

[1] Jaeger, Trent, Operating System Security, Morgan & Claypool Publishers, 2008, ISBN 9781598292121

[2] Operating System Concepts, Abraham Silberschatz, Peter B. Galvin, Greg Gagne, Wiley; 10th edition (2018)

[3] Ross Anderson, Security Engineering. Wiley. Around 600 pages covering real security issues and technologies. Not limited to computer or network security, it also covers psychology, economics, political and legal issues in depth. Not as much theory as other books, and relatively good to read if you have some basic knowledge of security. Some chapters can be freely downloaded from the website. (optional)

Other Resources

1. AWS Cloud Free Tier
2. Ubuntu Linux (www.ubuntu.org)
3. VmPlayer (www.vmware.com)

Reference Resource(s)

[1] Canadian Charter of Rights and Freedoms [online]. [Ottawa]: Department of Justice, 17 April 1982 [cited 27 January 2006]. Available from World Wide Web: http://laws.justice.gc.ca/en/charter/index.html.

[2] Criminal Code [online]. [Ottawa]: Department of Justice, 31 August 2004 [cited 27 January 2006]. Available from World Wide Web: http://laws.justice.gc.ca/en/C-46/index.html.

[3] Department of Defense Directive 8500.1: Information Assurance [online]. [Washington, District of Columbia]: Department of Defense, 24 October 2002 [cited 25 January 2006]. Available from World Wide Web: http://www.dtic.mil/whs/directives/corres/html2/d85001x.htm.

[4] Financial Administration Act [online]. [Ottawa]: Department of Justice, 31 August 2004 [cited 24 January 2006]. Available from World Wide Web: http://laws.justice.gc.ca/en/F-11/index.html.

[5] Government of Canada – Federated Architecture – Iteration One [online]. [Ottawa]: Treasury Board of Canada Secretariat, June 2000 [cited 1 April 2006]. Available from World Wide Web:

[6] Government of Canada – Information Infrastructure Protection: Vulnerability

Assessment – Concept of Operations. Final version 3.0. [Ottawa]: Communications Security Establishment, 7 December 2005. CSEC requisition W2213-6-0051, Contract Data Requirements List (CDRL) EN-01. Available from Treasury Board of Canada Secretariat (TBS) SiteScape Forum:

https://tbs-sct.scc.ca/tbs- sct/dispatch.cgi/f.gocpkitfnew/AVFLoginForm.

[7] William A. Arbaugh, David J. Farbert, Jonathan M. Smith, "A Secure and Reliable Bootstrap Architecture" http://www.cs.umd.edu/~waa/pubs/oakland97.pdf

[8] "DRAFT Role Based Access Control Implementation Standard", Version 0.1, NIST, January 2006 http://csrc.nist.gov/rbac/draft-rbac-implementation-std-v01.pdf

[9] Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller,"Krberos: An Authentication Service for Open Network Systems" Proceedings of the USENIX Winter 1988 Technical Conference.

[10] Steven M. Bellovin, Michael Merritt, "Limitations of the Kerberos

[11] Authentication System", ACM SIGCOMM Computer Communication Review, Volume 20, Issue 5 (October 1990), Pages: 119 – 132.

[12] http://www.cs.columbia.edu/~smb/papers/kerblimit.usenix.pdf

[13] Thomas Wu, "A Real-World Analysis of Kerberos Password Security", Proceedings of the 1999 ISOC Symposium on Network and Distributed, February 1999.

[14] http://www.passwordresearch.com/papers/paper21.html

[15] Gary Bahadur, Chris Weber, "Windows® XP Professional Security," McGraw-Hill, 2002, ISBN: 0072226021.

[16] Mann, Ellen Mitchell, Mitchell Krell, "Linux System Security: The Administrator's Guide to Open Source Security Tools," Scott 2nd Edition. Prentice Hall, 2002. ISBN: 0130470112

[17] Real World Linux Security, Bob Toxen, 2nd Edition, Prentice Hall, 2002, ISBN: 0130464562

[18] "UNIX System Security: A Guide for Users and System Administrators," Addison-Wesley, 1994, ISBN 0-201-56327-4

[19] Andrew Tanenbaum, "Modern Operating Systems," Second Edition, Prentice Hall, 2001, ISBN 0-13-031358-0

[20] Ross J. Anderson, Ross Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley, 2001, ISBN: 0471389226

[21] Matt Bishop, "Computer Security: Art and Science," Addison-Wesley Professional; 1st edition, 2002 ISBN: 0201440997

[22] Matt Bishop, "Computer Security: Art and Science," Addison-Wesley Professional; 1st edition, 2002 ISBN: 0201440997

[23] Oracle Autonomous Linux: https://www.oracle.com/ca-en/linux/autonomous-linux/

[24] NIST – Security and Privacy Controls for Information Systems and Organizations Publication 800-53, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[25] NIST – Mobile Device Security, Publication 1800-21, Sept 2020, https://csrc.nist.gov/publications/detail/sp/1800-21/final

[26] Mobile Security Reference architecture, US Department of Homeland Security, May 23, 2013 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf

[27] Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Feb 2019, https://www.nist.gov/publications/guide-attribute-based-access-control-abac-definition-and-considerations-1

[28] HIPAA 2014 - Waking Up the C-Suite to Privacy and Security Risks, https://csrc.nist.gov/CSRC/media/Presentations/HIPAA-2014-Waking-Up-the-C-Suite-to-Privacy-and/images-media/solove_hipaa_2014_day2.pdf

[29] Draft NIST Special Publication 800-216, Recommendations for Federal 3 4 Vulnerability Disclosure Guidelines, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216-draft.pdf

[30] NIST Special Publication 800-207, Zero Trust Architecture; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[31] NIST Special Publication 800-37, Revision 2; Risk Management Framework for Information Systems and Organizations; A System Life Cycle Approach for Security and Privacy; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[32] NIST Special Publication 800-6, Revision 2, Computer Security Incident Handling Guide; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Grading Guidelines

The final grade for the course will be calculated using the following grading scale:

Instrument		Percentage of Total Grade Revised
Class participation & Discussions		20
Projects		30
Midterm Exam		10
Final Exam		20
Quizzes		20
TOTAL		**100**

Attendance Policy

Students are expected to attend every class session. Instructors will inform students of the exact

number of absences and late-arrivals permitted during the semester. Students who exceed these limits may be subject to failure. If a student misses any class or test, the instructor has the right to either grant or deny an opportunity to make up the work that was missed. In such cases, the instructor shall be the sole judge of the validity of a student's explanation for having missed the class or test.

Deductions for Late Arrival, Early Departure, and Unexcused Absences

At the instructor's discretion, there will be point deductions for Late Arrival, Early Departure, and Unexcused Absences.

Policy for Make-Up Assignments or Quizzes

Make ups are allowed only in case of excused and documented absences. There are no exceptions.

Classroom Behavior

Behavior that disrupts, impairs, interferes with, or obstructs the orderly conduct, processes, and functions within an academic classroom or laboratory violates the student code of conduct and may result in disciplinary action. This includes interfering with the academic mission of NYIT or individual classroom or interfering with a faculty member's or instructor's role to carry out the normal academic or educational functions of his classroom or laboratory, including teaching and research.

Students with Physical or Educational Challenges:

- It is the policy of New York Institute of Technology to provide reasonable accommodations for students who are otherwise qualified but have disabilities, including learning disabilities, health impairments, and other disabling conditions. Possible accommodations include, but are not limited to, test schedule modifications, class relocation, and possible assistance in acquisition of necessary equipment.
- The college has an interest in helping students with disabilities to be competitive in this academic environment. Therefore, reasonable accommodations will be made upon proof both of disability and need for the accommodations. It must be understood that accommodations are meant to facilitate educational opportunities. Admission to NYIT and accommodations do not guarantee success. Therefore, in addition to accommodations, the college encourages utilization of auxiliary services available to all students to maximize opportunities for success. Students whose disabilities may require some type of accommodation must complete a request for accommodations form and an intake interview with their campus services coordinator prior to the academic semester. Accommodations maybe requested at any time during the semester; however, accommodations cannot be applied to past failures, only to future academic endeavors. Appropriate modifications of accommodations will be worked out on a case-by-case basis and will not necessarily incorporate all requested changes.

- Students for whom auxiliary services—such as readers, interpreters, note takers, etc.—have been approved should arrange these with their campus services coordinator. In addition to discussing appropriate educational modifications, the campus services coordinator will serve as a liaison with other college faculty and administration on behalf of students with disabilities.

Academic Integrity:

- Each student enrolled in a course at NYIT agrees that, by taking such course, he or she consents to the submission of all required papers for textual similarity review to any commercial service engaged by NYIT to detect plagiarism. Each student also agrees that all papers submitted to any such service may be included as source documents in the service's database, solely for the purpose of detecting plagiarism of such papers.
- Plagiarism is the appropriation of all or part of someone else's works (such as but not limited to writing, coding, programs, images, etc.) and offering it as one's own. Cheating is using false pretenses, tricks, devices, artifices or deception to obtain credit on an examination or in a college course. If a faculty member determines that a student has committed academic dishonesty by plagiarism, cheating or in any other manner, the faculty has the academic right to 1) fail the student for the paper, assignment, project and/or exam, and/or 2) fail the student for the course and/or 3) bring the student up on disciplinary charges, pursuant to Article VI, Academic Conduct Proceedings, of the Student Code of Conduct. The complete Academic Integrity Policy may be found on various NYIT Webpages, including: http://www.nyit.edu/images/uploads/academics/AcademicIntegrityPolicy.pdf.

Using the NYIT Library

- All students can access the NYIT virtual library from both on and off campus at www.nyit.edu/library. The same login you use to access NYIT e-mail and NYITConnect will also give you access to the library's resources from off campus.

- On the left side of the library's home page, you will find the "Library Catalog" and the "Find Journals" sections. In the middle of the home page you will find "Research Guides;" select "Video Tutorials" to find information on using the library's resources and doing research.

- Should you have any questions, please look under "Library Services" to submit a web-based "Ask-A-Librarian" form.

Weekly Topical Class Schedule

DAYS	Topic	Reading	Assignments	Due Date
1	Introduction & Orientation: Overview of Operating Systems Cloud Introduction – Pointers to Tutorials **Lab 1** – Hands-on work Introduction to Unix/Linux	[2] Ch. 1		Day 3
2	Secure Operating Systems, Basic Concepts in Information Security, Threats to a Secure Operating System Access Matrix, Implementation of Access Matrix, Access Control, Revocation of Access Rights, Capability-Based Systems, Language-Based Protection QUIZ #1	[1] Ch. 1 [2] Ch. 14		
	Project 1 Environment Variable and SetUID The Objective: To understand how environment variables affect program and system behaviors. Includes hands-on activities to demonstrate learning.			Day 5
3	The Security Problem, Program Threats; System and Network Threats, cryptography as a Security Tool, User Authentication, Implementing Security Defenses, Firewalling to Protect Systems; Computer-Security Classifications	[2] Ch. 15 Lecture Notes		
4,5	Access Control Fundamentals: Protection Systems, Mandatory Protection Systems, Reference Monitors, Definition of a Secure Operating System, Assessment criteria to be used against each operating system.	[1] Ch.2		
	Project 1; Select Presentations QUIZ #2			
6	Security in Ordinary Operating Systems: Unix and Windows **Project 2** Race Condition type project.	[1] Ch 3 [2] Ch 15		Day 8

	Lab Presentations			
7,8	Goals of Protection, Principles of Protection, Domain of Protection, Confidentiality vs Integrity Verifiable Security Goals: Information Flow Confidentiality Models, Information Flow & Integrity Models Introduction	[2] Ch 14, [1] Ch 5		
	Project 3 – OS Vulnerabilities – VM Hardening OS Security in Cloud MIDTERM		**Hands on**	Day 12
9,10	BLP & Biba Model, Covert Channels: types and controls	[1] Ch 5		
	MIDTERM REVIEW			
11,**12**	Securing Commercial Operating Systems Runtime Containers Security OS Support for Cryptography Symmetric-Key Cryptography, Traditional Ciphers	[1] Ch 7, Ch9 Lecture Notes		
	Select Project 3 Presentations QUIZ #3			
13,14	Data Encryption Standard (DES), Public-key Cryptography, RSA**,** Symmetric Key Encryption, Public Key Encryption, Certificates, Digital Signatures using OpenSSL	Lecture Notes & [1] Ch. 9		
	Select Project Presentations/Review Review, Questions and Answers / Reflections			
15	FINAL EXAM			