Course Outline

695.744 Spring '22

T. McGuire
Johns Hopkins University

This outline provides an overview of the course and assignments by week. Please remember to check the calendar for specific due dates and Blackboard for specific reading material, reading assignments, and problem sets.

Each course module runs for a period of seven (7) days, i.e. one week from a Monday to a Sunday. Due dates for readings and other assignments are 11:59 PM Eastern on the last day of the module, unless noted otherwise. Please check Blackboard for most up-to-date information.

Note: Readings in blue are optional. **See the content module for up-to-date information**.

IMPORTANT: PLEASE CHECK THE ADDITIONAL READING SECTION BELOW. IT CONTAINS URLS FOR THE JHU SHERIDAN LIBRARY THAT HAS SOME OF THE BOOKS FOR OPTIONAL READINGS.

Module	Dates	Topics	Assignments
1	1/24 - 1/30	Introduction to Intel Assembly	Reading: PDF Readings Lecture Videos Ch. 4 - Practical Malware Analysis Ch. 1 - Practical Reverse Engineering Ch. 1 - Reversing: Secrets of Reversing Homework: Assignment 1 Discussions: Introduction Discussion 1
2	1/31 - 2/6	Disassembly Process Revealed	Reading: PDF Readings Lecture Videos Ch. 1 - The IDA Pro Book Ch. 2 - Reversing: Secrets of Reversing Homework: **Project 1 - Due at end of Module 4** Discussions: Discussion 2
3	2/7 - 2/13	Errors, Errors, Everywhere	Reading: PDF Readings Lecture Videos Ch. 4 - Reversing: Secrets of Reversing Ch. 5/6 - The Art of Software Security Assessment Homework: Assignment 2 Continue Project 1 Discussions: None
4	2/14 - 2/20	Source Code Analysis	Reading: PDF Readings Lecture Videos Ch. 5/6 - The Art of Software Security Assessment Homework: **Complete Project 1** Discussions: Discussion 3
5	2/21 - 2/27	Binary Analysis	Reading: PDF Readings Lecture Videos Homework: Assignment 3 Discussions: Discussion 4

Module	Dates	Topics	Assignments
6	2/28 - 3/6	Blind Binary Analysis	Reading: PDF Readings Lecture Videos Ch. 4 - Reversing: Secrets of Reversing Homework: Assignment 4 **Prepare for Midterm** Discussions: None
7	3/7 - 3/13	Midterm	Reading: None Homework: **Midterm** Discussions: None
8	3/14 - 3/20	Debugging Demystified	Reading: PDF Readings Lecture Videos Homework: Assignment 5 Discussions: Discussion 5
Break	3/21 - 3/27		Reading: None! Homework: None! Discussions: None!
9	3/28 - 4/3	Protection Mechanisms	Reading: PDF Readings PowerPoint Slides Lecture Videos Ch. 3 - Reversing: Secrets of Reversing Homework: Assignment 6 Discussions: Discussion 6
10	4/4 - 4/10	ROP and SEH	Reading: PDF Readings PowerPoint Slides Lecture Videos Ch. 3 - Reversing: Secrets of Reversing Homework: Assignment 7 Discussions: None

Module	Dates	Topics	Assignments
11	4/11 - 4/17	OS Internals and Introductory Malware Analysis	Reading: PDF Readings Lecture Videos Homework: **Project 2 - Due at end of Module 12** Discussions: None
12	4/18 - 5/24	Advanced Malware Analysis	Reading: PDF Readings Practical Analysis Lecture Videos Ch. 10 - Practical Malware Analysis Ch. 3 - Practical Reverse Engineering Homework: **Complete Project 2** Discussions: Discussion 7
13	4/25 - 5/1	Science and Art of Fuzzing	Reading: PDF Readings Lecture Videos Ch. 2/3 - Fuzzing: Brute Force Vulnerability Discovery Homework: Assignment 8 **Prepare for Final Exam** Discussions: None
14	5/2 - 5/8	Advanced Reverse Engineering Topics and Final Exam	Reading: PDF Readings Lecture Videos Homework: **Final Exam** Discussions: None

Additional Reading Resources

- The Art of Software Security Assessment. Mark Dowd, John McDonald, Justin Schuh

  https://learning.oreilly.com/library/view/the-art-of/0321444426/

- Practical Malware Analysis. Michael Sikorski

  https://learning.oreilly.com/library/view/practical-malware-analysis/9781593272906/

- Reversing: Secrets of Reverse Engineering. Eldad Eilam

  https://learning.oreilly.com/library/view/reversing-secrets-of/9780764574818/

- Fuzzing: Brute Force Vulnerability Discovery. Michael Sutton, Adam Greene, Pedram Amini

  https://learning.oreilly.com/library/view/fuzzing-brute-force/9780321446114/

- Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools and Obfuscation. Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sebastien Josse.

  https://learning.oreilly.com/library/view/practical-reverse-engineering/9781118787397/

- Intel 64 and IA-32 Architectures Software Developer's Manuals.

  http://www.intel.com/products/processor/manuals/

- X86 Assembly Language and C Fundamentals. Joseph Cavanagh

  https://learning.oreilly.com/library/view/x86-assembly-language/9781466568259/

- Computer Systems: A Programmer's Perspective, 2nd ed. Randal Bryant.

- A Guide to Kernel Exploitation: Attacking the Core. Enrico Perla and Massimiliano Oldani.

  https://learning.oreilly.com/library/view/a-guide-to/9781597494861/

- The Ghidra Book. Chris Eagle, Kara Nance

  https://learning.oreilly.com/library/view/the-ghidra-book/9781098125684/

- The IDA Pro Book: Second Edition. Chris Eagle

  https://learning.oreilly.com/library/view/the-ida-pro/9781593273750/

- Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection. Jasvir Nagra

  https://learning.oreilly.com/library/view/surreptitious-software/9780321591258/

- Secure Programming with Static Analysis. Brian Chess, Jacob West

  https://learning.oreilly.com/library/view/secure-programming-with/9780321424778/

- Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. Alex Matrosov, Eugene Rodionov, Sergey Bratus

  https://learning.oreilly.com/library/view/rootkits-and-bootkits/9781492071259/

- Smashing the stack for fun and profit. Aleph One

  http://insecure.org/stf/smashstack.html

- Nathan E. Rosenblum, Xiaojin Zhu, Barton P. Miller, and Karen Hunt, "Learning to Analyze Binary Computer Code", 23rd Conference on Artificial Intelligence (AAAI-08), Chicago, Illinois, July 2008.

  ftp://ftp.cs.wisc.edu/paradyn/papers/Rosenblum08aaai.pdf

- Nathan E. Rosenblum, Xiaojin Zhu, Barton P. Miller, and Karen Hunt, "Machine Learning-Assisted Binary Code Analysis", NIPS 2007 Workshop on Machine Learning in Adversarial Environments for Computer Security, Vancouver, British Columbia, Canada, December 2007.

  ftp://ftp.cs.wisc.edu/paradyn/papers/nips07-abs.pdf

Various research papers related to binary code auditing, source code auditing, fuzzing, and protection mechanisms to prevent exploitation.