Course Student Learning Outcomes
Upon successful completion of this course, students will be able to demonstrate the following competencies:

- **LO1.** Describe major classes of and techniques for software system analysis (**knowledge**);
- **LO2.** Select and apply static analysis techniques to software systems (**application**);
- **LO3.** Select and apply dynamic analysis techniques to software systems (**application**);
- **LO4.** Develop test code and testing frameworks for understanding and defending against software exploits (**synthesis**);

Program Student Outcomes supported by this class
This course directly supports the following program student outcomes in the CYB program assessment and improvement plan:

- **SO1.** Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
- **SO2.** Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
- **SO6.** Apply security principles and practices to maintain operations in the presence of risks and threats.

Assignments / Assessments of Course Student Learning Outcomes
Learning outcomes are assessed through a variety of means: Assignments, forum threads, and a final exam assess a student's ability to describe and explain foundational concepts in software analysis (LO1) and specific analysis and testing techniques and concepts (LO2-LO4).

Individual and team homework assignments assess student ability to synthesize and analyze software systems, secure-design methods, and problem-solving. Key homework assignments will include: building and walking annotated CFG (LO2), using afl-fuzz and Deep State as part of a formal and stochastic testing approaches (LO3), and using a combination of techniques as part of a testing and security strategy for software (LO4).

Class participation is an integral part of the class.

Discussion forums will be a part of your participation grade. There will be a prompt each week, with a specific, rubric-driven requirement for participation. There will also be a separate general participation grade that is focused on participation in a professor-lead discussion that will introduce the week's content in an interactive (though asynchronous) fashion. The participation grade may also factor in (positively) personal interaction with the professor and other contributions.

Discussion Board Forums

Students are expected to post to each discussion board with appropriate responses. Proper etiquette is expected in discussion boards- this includes grammar, spelling, etc, and also includes treating your classmate and his/her ideas with respect. It is proper to give constructive ideas and criticisms, however it will not be acceptable to give improper or childish responses to another's ideas. A discussion rubric will be provided on the course website for grading. Each week, unless otherwise noted, you are expected to post your response to the question by Wednesday, 11:59pm (Flagstaff time) and you are expected to respond to two classmates by Sunday, 11:59pm (Flagstaff time).

Grading System

A weighted sum of assessment components is used to determine your final grade in the course:

- Discussion Boards: **10% (weekly prompts)**
- Participation in "Class Time Thread": **10% for participation in the weekly content thread**
- Homework assignments (3): **60%**
- Final Exam: **20%**

Grades will be assigned using the weighted sum described above using this scale:
A ≥ 90%, **B** ≥ 80%, **C** ≥ 70%, **D** ≥ 60%, **F** < 60%.

There is no "curve". Each student's grade is based on their own outcomes assessments and not affected by the grades of other students. Extra credit opportunities may present themselves throughout the semester and will be announced during class meetings. Mistakes in grading to happen, and students are encouraged to discuss such concerns with the instructor during office hours.

Readings and Materials

Readings come from research papers and chapters freely available online:

Week 1

Anderson Chapter 1: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf
(Optional Readings):
http://heartbleed.com/
https://blog.cryptographyengineering.com/2014/04/08/attack-of-the-week-openssl-heartbleed/
https://www.imperialviolet.org/2014/02/22/applebug.html
https://opensource.apple.com/source/Security/Security-55471/libsecurity_ssl/lib/sslKeyExchange.c

Week 2

Anderson Chapter 3: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c03.pdf
(Optional Readings):
Lowe, "Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR": https://www.cs.utexas.edu/~shmat/courses/cs6431/lowe.pdf

Week 3

Chess and McGraw, "Static Analysis for Security":
https://www.garymcgraw.com/wp-content/uploads/2015/11/bsi5-static.pdf

Week 4

Bonus static analysis reading:
https://cacm.acm.org/magazines/2010/2/69354-a-few-billion-lines-of-code-later/fulltext (one of the best articles on real-world static analysis, with some amusing and deep insights)

Week 5

Discussion of python tools:
https://blog.codacy.com/review-of-python-static-analysis-tools-ff8e7e27f972 (2016)
https://blog.codacy.com/which-python-static-analysis-tools-should-i-use/ (2018)

Week 6

Holzmann (my boss at JPL, inventor of the SPIN Model Checker) on his static analysis tool:
http://www.spinroot.com/uno/uno_long.pdf

Week 9

Miller's famous fuzzing paper:
ftp://ftp.cs.wisc.edu/paradyn/technical_papers/fuzz.pdf
Lagorio, "Introduction to fuzzing using American Fuzzy Lop"
https://bart.disi.unige.it/zxgio/phd-course-2017/fuzzing_slides.pdf
Gaynor, "Introduction to Fuzzing in Python with AFL"
https://alexgaynor.net/2015/apr/13/introduction-to-fuzzing-in-python-with-afl/

Week 10

Regehr, How to Fuzz an ADT Implementation
https://blog.regehr.org/archives/896
Groce, Fuzzing an API with DeepState, Parts I and II:
https://blog.trailofbits.com/2019/01/22/fuzzing-an-api-with-deepstate-part-1/

Week 11

Edward J. Schwartz, Thanassis Avgerinos, David Brumley, "All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask)"
https://users.ece.cmu.edu/~aavgerin/papers/Oakland10.pdf
Go back and read "Coverage and its Discontents"
https://agroce.github.io/onwardessays14.pdf

Week 12

Bug Hunter's Diary, Chapters 1 and 2
http://index-of.es/Networking/Bug%20Hunter%20Diary.pdf

Week 13

Bug Hunter's Diary, Chapter 7
http://index-of.es/Networking/Bug%20Hunter%20Diary.pdf

Week 14

SQL injection detection via dynamic analysis:
https://hiper.cis.udel.edu/lp/lib/exe/fetch.php/courses/issta08-wassermann-testgenweb.pdf

Week 15

(Optional Readings):
Anderson chapter 17: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c17.pdf
Heavy duty reading on state-of-the-art static analysis responses:
https://pdfs.semanticscholar.org/5fd4/7722da2f900b94cdaf313e8148658ceefef7.pdf

Students will also need access to a computer with the following software tools:

- GCC suite; Python
- VirtualBox or VMWare to access Linux
- In place of VMWare, Docker will also work, in fact work better!

Class Outline and Tentative Schedule

The course topics and a tentative schedule serve as an outline for the class:

	Dates	Topics	Reading	Assignment
Week 1	8/12-8/16	Intro to Software Security (CIA)	Anderson Ch 1	TH1 DB1
Week 2	8/17-8/23	Protocols	Anderson Ch 3	TH2 DB2 HW1, 1(3)
Week 3	8/24-8/30	Static analysis basics (part 1)	Chess & McGraw, Video	TH3 DB3 HW1, 2(3)
Week 4	8/31-9/6	Static analysis basics (part 2)	Bonus Static Analysis	TH4 DB4 HW1, 3(3)
Week 5	9/7-9/13	Python tools for static analysis	Codacy Review	TH5 DB5
Week 6	9/14-9/20	Building static analysis tools (part 1)	Holzmann, Video	TH6 DB6 HW2, 1(4)
Week 7	9/21-9/27	Building static analysis tools (part 2)		TH7 DB7 HW2, 2(4)
Week 8	9/28-10/4	Building static analysis tools (part 3)		TH8 DB8
Week 9	10/5-10/11	afl-fuzz	Miller, Lagorio, Gaynor, Video	TH9 DB9 HW2, 3(4) HW2, 4(4)
Week 10	10/12-10/18	DeepState symbolic unit testing	Regehr, Groce	TH10 DB10
Week 11	10/19-10/25	Hybrid testing approaches	Schwartz, Video	TH11 DB11
Week 12	10/26-11/1	Building exploits	BHD 1-2	TH12 DB12 HW3, 1(4)
Week 13	11/2-11/8	Common exploit classes	BHD 7	TH13 DB13 HW3, 2(4)
Week 14	11/9-11/15	SQL injection attacks	SQL	TH14 DB14 HW3, 3(4) HW3, 4(4)
Week 15	11/16-11/22	Advanced topics; next steps		TH15 DB15
Week 16	11/23-11/25	**Final exam**		**Final exam**

TH= Class Time Thread DB= Discussion Board HW=Homework Assignment

semester to activate their approved accommodations. Although a student may request an accommodation at any time, it is best to initiate the application process at least four weeks before a student wishes to receive an accommodation. Students may begin the accommodation process by submitting a self-identification form online at https://nau.edu/disability-resources/student-eligibility-process or by contacting Disability Resources. The Director of Disability Resources, Jamie Axelrod, serves as NAU's Americans with Disabilities Act Coordinator and Section 504 Compliance Officer. He can be reached at jamie.axelrod@nau.edu.

RESPONSIBLE CONDUCT OF RESEARCH

Students who engage in research at NAU must receive appropriate Responsible Conduct of Research (RCR) training. This instruction is designed to help ensure proper awareness and application of well-established professional norms and ethical principles related to the performance of all scientific research activities. More information regarding RCR training is available at https://nau.edu/research/compliance/research-integrity.

MISCONDUCT IN RESEARCH

As noted, NAU expects every student to firmly adhere to a strong code of academic integrity in all their scholarly pursuits. This includes avoiding fabrication, falsification, or plagiarism when conducting research or reporting research results. Engaging in research misconduct may result in serious disciplinary consequences. Students must also report any suspected or actual instances of research misconduct of which they become aware. Allegations of research misconduct should be reported to your instructor or the University's Research Integrity Officer, Dr. David Faguy, who can be reached at david.faguy@nau.edu or 928-523-6117. More information about misconduct in research is available at https://nau.edu/university-policy-library/misconduct-in-research.

SENSITIVE COURSE MATERIALS

University education aims to expand student understanding and awareness. Thus, it necessarily involves engagement with a wide range of information, ideas, and creative representations. In their college studies, students can expect to encounter and to critically appraise materials that may differ from and perhaps challenge familiar understandings, ideas, and beliefs. Students are encouraged to discuss these matters with faculty.

Last revised XX, 202

Syllabus Updated 8/25/2021