CS 491/591 Reverse Engineering, Spring 2016

Instructors: Carrie Jung, Bob Jung, and Jed Crandall

Instructor of record: Jed Crandall, crandall@cs.unm.edu

PGP info is on my website: https://www.cs.unm.edu/~crandall

Never hesitate to email Jed directly about anything.

Office and office hours: FEC 335, Mondays and Wednesdays from 1:30pm to 3:00pm, or by appointment.

Class meeting time and place: MW from 11:00am to 12:15pm, in CEC B146 (the lab in the basement of the Centennial Engineering Center). Attendance will not be recorded and will not be explicitly part of your grade, but we strongly encourage you to attend class regularly because we're going to move at a fast pace.

Prerequisites: None formally, having taken CS 341 (Computer Organization and Design) or an equivalent class plus CS 444/544 (Intro to Cybersecurity) or an equivalent class before taking this class is recommended. You should be familiar with concepts like assembly language, system calls, virtual memory, symmetric and asymmetric cryptography, hash functions, *etc.* before taking this class. We will not be reviewing these concepts.

Mailing lists: There are two mailing lists, one required and one optional. See the course website for details.

Course website: http://www.cs.unm.edu/~crandall/respring16/

We'll post lots of important stuff here, like the lab assignments, links to the mailing lists, *etc.*

Required text: Practical Malware Analysis, by Michael Sikorski and Andrew Honig. (https://www.nostarch.com/malware)

Grading: The final grade will be calculated as 50% labs, 25% homeworks, and 25% semester project. The points for each will be added up and divided into the total possible before weighting, so a 100-point lab does not *necessarily* contribute ten times the amount to your grade as a 10 point homework. We reserve the right to curve the overall grades at the end of the semester (up, never down) if we don't feel that they reflect the amount of effort students put into the class. The overall grade will be out of 100, weighted as described above. For letter grade purposes, below 60 is an F, 60 and up is a D, 65 and up is a C-, 70 and up is a C, 75 and up is a C+, 80 and up is a B-, 82 and up is a B, 85 and up is a B+, 87 and up is an A-, and 90 and up is an A. We only give A+'s in extreme circumstances.

Note: The grading standard on the semester project will be different for undergraduates (CS 491) and graduates (CS 591).

Labs: There will be 3 labs, all weighted equally. How each lab gets graded will be written on the lab assignment.

Be sure to start early on the lab assignments and get the help you need to get them done.

Late assignments will be accepted only in special circumstances (medical, *etc.*).

For lab writeups, English spelling and grammar may affect your grade, since it's very difficult for us to

read---and therefore also difficult for us to understand---English writing that has poor grammar. There are various University resources for helping students with English writing, contact Jed if you need help finding these resources.

Homeworks: There will be about fifteen to twenty relatively light homework assignments throughout the semester.

Midterm and final: There will be no midterm or final exam.

Semester project: More details will be outlined later about the semester project. It'll be self-guided and fairly open in terms of what you choose to work on.

UNM statement of compliance with ADA: "Qualified students with disabilities needing appropriate academic adjustments should contact the professor as soon as possible to ensure your needs are met in a timely manner. Students must inform the professor of the disability early in the class so appropriate accommodations can be met. Handouts are available in alternative accessible formats upon request."

Cheating and collaboration, personal statements:

Every homework assignment and lab assignment, unless we specify otherwise, should be an individual effort where you do your own work and only discuss the assignment with your classmates at a high level.

Each lab will have a special section of the assignment writeup where we'll try to be as specific as possible about what is allowed or not allowed with respect to cheating and collaboration. In general, you are expected to do your own work, and for group work all group members are expected to contribute.

If you copy and paste any material (English text, figures, etc.) from any source you must clearly delineate it and attribute it properly to its source. Representing the work and materials of others as your own will not be tolerated in this class. Anything that is a full sentence or more that was not written originally by you has to be in quotes or indented in italics with a reference to clearly indicate where the material came from. Even if it was an accident, any kind of plagiarism in this class will result in an F in the class and possibly further actions pursuant to UNM policy.

All university policies regarding these matters will be strictly enforced. Typically we'll give the cheating parties an F in the class, but we may pursue further action in some cases.

As per University policy, grades of "Incomplete" or "Withdrawal", changes in grade mode, or any other special accommodations will only be considered in cases where circumstances arose that were outside the control of the student (such as a death in the family, medical issues, etc.). Losing a scholarship or visa status because of a low grade is a very serious issue, but it's up to you to do well in the classes you register for to make sure that doesn't happen, not up to the instructors of the classes you take.

Some lab assignments *may* be group efforts. We expect everybody to contribute, if some group members do all the work and others slack off, we consider that a fault of each and every member of the group individually. Doing all the work yourself is not an alternative to showing leadership.

Our expectations of you as students

- **Be studious:** We expect students to come to class, to come on time, to stay on task, to take the time to make sure they understand things well, *etc*.
- **Do only excellent work:** anything worth doing is worth doing well. Keep your projects and writing simple and make sure everything you do is excellent and technically sound. Especially for the semester project, don't bite off more than you can chew.

- **Show leadership and be a mentor:** don't think that this class is only about reverse engineering. We may not do group assignments in this class, but you'll be working with people throughout the semester and if someone is not as strong as you are in reverse engineering or programming, help them learn and motivate them to get things done instead of doing everything yourself.
- **Take responsibility for your own learning:** you're either registered for a 400-level class or for a graduate class, at a major research institution. If you find that coming to the regularly scheduled class time is a waste of time, then you're probably not taking responsibility for your own learning. Don't expect us to spoon-feed you information that is already well-known, you don't want to pay ~$750 in tuition for us to tell you what's in a ~$60 textbook that you could read yourself if you wanted to. Our job is to help you help yourself to learn. A good philosophical approach for you to take in this class is to "teach the teacher."

Material to be covered:

Basic static analysis, safe environment, basic dynamic Analysis, x86, IDA Pro, C constructs, Windows internals, debugging, OllyDbg, covert malware launching, malware behavior, data encoding and encryption, network signatures, anti-disassembly, anti-debugging, anti-VM, packers, shellcode analysis, machine learning (classification and clustering), information theory (including Kolmogorov complexity), academic studies of malicious code such as viruses and worms, cryptovirology, attacks on both symmetric and asymmetric ciphers, random number generation, virtualization, advanced computer architecture (*e.g.*, concurrency issues of trace caches), network intrusion detection system evasion, and societal impact and legal issues.

If you have a specific interest you'd like us to talk about in class or you have any other suggestions for lectures or class discussions, please let us know.

The class will also have a heavy focus on societal impact issues, which will be part of the labs and homeworks and will also be discussed regularly in class. These issues will include laws and regulations in the U.S. and overseas related to reverse engineering, University policy, Internet surveillance, Internet censorship, and ethical disclosure of vulnerabilities. If any material or assignments make you uncomfortable (*e.g.*, because of possible repercussions for you in the country of your citizenship or at your job) please let us know.

Ethical scholarship and proper use of UNM resources

You're responsible for understanding the laws and UNM policies pertaining to everything we do in class. We'll cover this early in the semester, including University polices 2500 and 2520, and privacy laws relevant to the use of Wireshark.