CS 212 – Assembly Language & Reverse Engineering

M. E. Kabay, PhD, CISSP-ISSMP, Prof of Computer Information Systems
School of Business & Management, Norwich University

1 Course Description

An introduction to assembly language and reverse engineering, including relationship among machine language, assemblers, disassemblers, compilers, and interpreters. This courses provides requisite skills for computer forensics, malware analysis, and cryptology. Prerequisites: 'C' or higher in IS 131 or CS 140.

All specifics of topics, schedule and deadlines are in the CS212 Syllabus.

2 Course Objectives

By the end of this course, students will be able to

- Use binary and hexadecimal numbering for representing and reading data;
- Describe the functions and attributes of registers, flags, and memory-based operands used in instructions;
- Describe how stack operations function;
- Describe functions of 80x86 assembler code elements;
- Describe architecture fundamentals of x86/x64 systems using appropriate terminology;
- Describe architecture fundamentals of ARM systems using appropriate terminology;
- Describe internals of the Windows kernel using appropriate terminology;
- Describe obfuscation and Deobfuscation concepts and terminology.

3 Course Schedule & Location

Section A: MWF in Dewey 206 from 10:00:03 – 10:49:57 and using NUoodle.
Section B: MWF in Dewey 211 from 11:00:03 – 11:49:57 and using NUoodle.

4 Course Textbooks

These texts have been ordered through the Norwich University bookstore.

Part 1 of the course: Detmer, R. C. (2015). *Introduction to 80x86 Assembly Language and Computer Architecture* (3rd ed.). Jones & Bartlett Learning. Retrieved Nov 16, 2016, from https://www.amazon.com/Introduction-Assembly-Language-Computer-Architecture/dp/128403612X/

Part 2 of the course: Dang, B., Gazet, A., & Bachaalany, E. (2014). *Practical Reverse Engineering: X86, X64, ARM, Windows Kernel, Reversing Tools, and Obfuscation* (1st ed.). Wiley. Retrieved Nov 16, 2016, from https://www.amazon.com/Practical-Reverse-Engineering-Reversing-Obfuscation/dp/1118787315/

5 Course Materials on NUoodle

Course materials including assigned readings, exercises, quizzes and supplementary references are posted online on the CS212 section on NUoodle.

6 Mechanics

- Classes will meet as stipulated in the syllabus. Attendance is mandatory; a record of attendance will be kept. More than three unexcused absences will result in expulsion from the course with an F grade.
- Readings, videos, and sound recordings (required and optional) are listed in the weekly assignments on NUoodle.
- Students should read, listen to or view specified assigned readings, audio recordings or videos before coming to class.

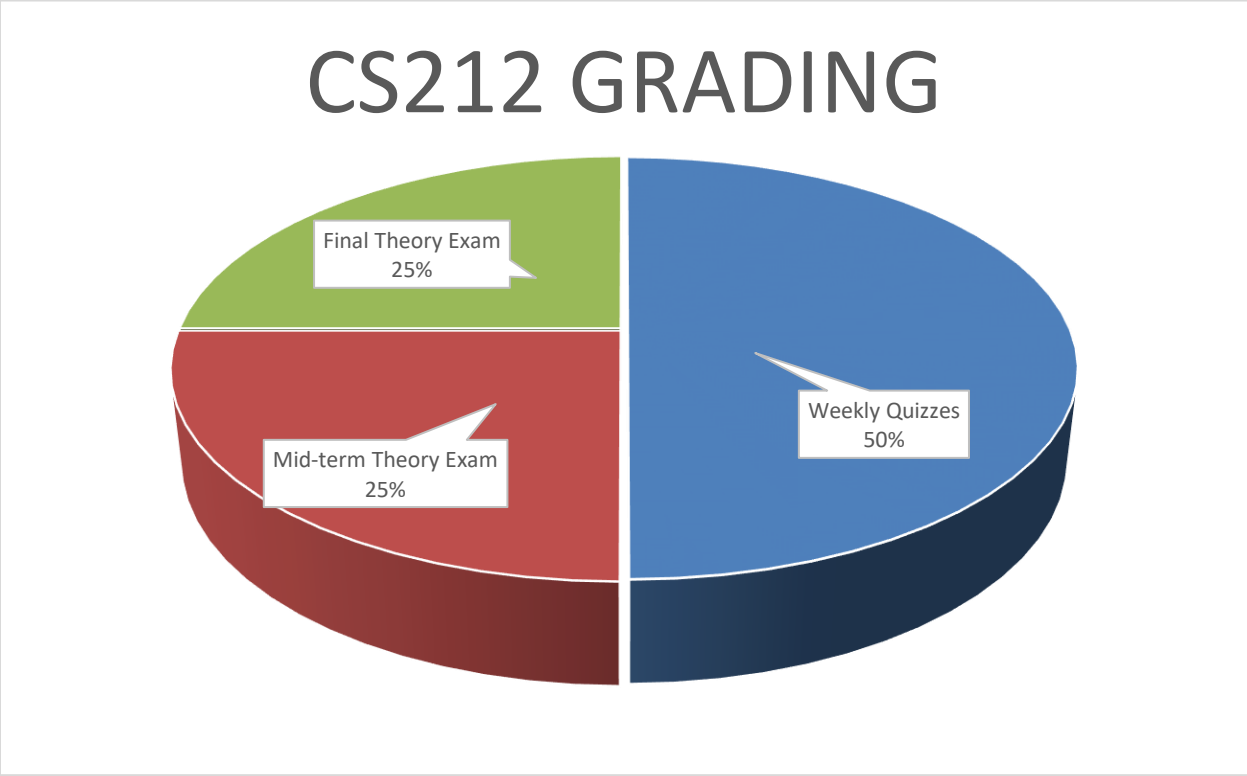
7 Methods of Assessment

All assignments and quizzes are submitted using NUoodle. Deadlines for each assignment are posted in NUoodle and on the class syllabus.

Responding punctually to professional responsibilities is part of the maturation of students. To encourage promptness, early submissions for any of the essay exams and assignments will result in bonus points of 1% per day for the total score allotted to the assignment. Late submissions are rejected and will result in scores of 0% for the exam.

For all NUoodle quizzes and exams, quizzes close at their deadlines and cannot be taken or retaken after closure.

The figure below shows the breakdown of elements of the final grade.



7.1 Weekly quizzes: 50% of final grade

Weekly online quizzes will close at 23:55 on the SUNDAY *two weeks* after the start of each week of study (which is also defined on Sundays). The quizzes will test familiarity with the concepts and terminology assigned in the corresponding week. All questions will be listed in the review questions posted weekly.

7.2 Mid-term Exam: 25% of final grade

The online mid-term exam will be based on the review questions for the first part of the course.

7.3 Final Exam: 25% of final grade

The online final exam will be based on the review questions for the second part of the course.

7.4 Extra-credit Work

Students may discuss extra-credit work with the instructor to define written specifications and points. Such work may consist of coding projects, written essays based on recent relevant professional articles (1 final % point per 500 words), demonstrations, in-class lectures, or other educational activities. The maximum total number of points available for any such work over the course of the semester is 10% points added to the final grade.

8 Cheating and Plagiarism

Students are graded on an individual basis and must therefore complete their own work. Students are reminded of the University's Policy against cheating and plagiarism:
< http://www.norwich.edu/about/policy/academic/appendix1.html >.

If in doubt as to what constitutes plagiarism, students should ask the instructor for a review of their work before submitting an assignment. All instances of cheating and of plagiarism must be reported to the Academic Integrity Committee by the instructor or by students who have observed the dishonesty. Penalties include expulsion from the University. Ignorance of the University's Rules is not a valid defense against accusations of academic dishonesty.

9 Attendance Policy

There must be no more than three unexcused absences from this course because it meets thrice a week.

University regulations stipulate that "Unless stated otherwise, the maximum number of permitted absences is the number of times the course meets per week. When the student has reached the maximum number of permitted absences, the faculty member will warn the student of impending dismissal from class with a grade of 'F.' This warning letter will include the course number and section and dates(s) of absence(s). The letter will state that any future unexcused absences may result in recommendation to the Vice President of Academic Affair through the course School Dean that the student be dismissed from the class with a grade of 'F.' A copy of the warning letter will go to the student's academic advisor and to the Commandant and Vice President of Student Affairs.' (See pp 69-70 of the PDF version of the *Academic Regulations* available online at < http://tinyurl.com/nuar2009 >.)

Thus, students may miss one, two or three sessions of this course without needing any explanation. If students *plan* to be absent, they should discuss the absence with the instructor in advance to be excused; after an absence, the instructor requires a written explanation for consideration. The fourth and subsequent unexcused absences will be reported as stipulated in the academic regulations and may lead to dismissal from the course with an F grade.

10 Policy on Electronic Distractions

Some students constructively use computers to take notes or to research discussion points to contribute to class sessions. However, some students have displayed immature and rude behavior by using their mobile phones, tablets, and laptop computers to access services such as online games, chat services, social-networking sites, or other services that have no value for the class discussions or for their own learning. Some of these students have distracted other students and irritated the instructor. Students must understand that divided attention does *not* improve learning.

Therefore, in this course, students are on notice that anyone using their electronic equipment (or for that matter, reading a novel, taking a sitz-bath, training a gerbil, or preparing breakfast on a camping stove) for non-class-related purposes will be expelled from the class and counted as absent. Anyone wishing to avoid embarrassment and potential humiliation will want to avoid such interactions with the instructor.

11 Office Hours & Contact Information:

Students are welcome to call the instructor at **(802) 479-7937** at *any time* (that number rings in his office or his cell phone but cannot disturb him at home); leave a voice-mail message with a return number if necessary. The same number may be used for SMS (text) messages. Similarly, Facebook texting using the Messenger app are accepted. Students are also encouraged to use Skype (ID is **mekabay**) and are also welcome to leave voice or video recordings using Skype. The instructor is almost always running Skype; the status icon turns yellow for away after five minutes of inactivity on his system.

Office hours are posted on the instructor's Website home page, class Web site, on NUoodle, and on the instructor's office door (Dewey 209). The **Dewey 209** office door is almost always open when the instructor is present; all students are most welcome to drop in without having to make appointments – everyone is welcome at any time. It is *not necessary to make and appointment* – the instructor welcomes visits and always responds to students with a cheery, "Hi! What can I do for you?" Many students have enjoyed cups of coffee or cocoa and some hungry people have even been fed emergency granola bars. Do come and visit!

12 Additional Notes

- There will be no *grading on a curve*. There are no predetermined numbers of final letter grades. Students do not compete with each other for grades; if everyone gets A, great. If everyone fails, tough – the evidence will support the results. Remember that NUoodle keeps detailed log files showing the exact timing and duration of visits to that service; it's hard to claim that a, say, 3% received as a final grade was unfair when the log files show that the student took exactly one quiz, refused to submit mid-term and final exams, and was online in NUoodle for a total of eight visits lasting a total of 22 minutes.
- Students are encouraged to study together, to help each other by reviewing code and making constructive suggestions for improvement, but not to collaborate in preparation of *exam* responses. Students do work in teams of four on their final project, as described in section **Error! Reference**

You are not required to read the biographical details on the next page.

They're available for any students who are curious about their instructor's professional background.

source not found..

13 More Than You Need or Want to Know About your Instructor

M. E. Kabay began teaching his high school classmates how to use the slide rule in 1963 (NOT the best way to become popular) and began programming IBM 1401 computers in assembly language in 1965, switching to FORTRAN IV G as fast as he could. He continued to program throughout his BSc & MSc studies at McGill University and used assembler for his HP programmable calculators throughout his studies. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology (?!?) and taught statistics (and a couple of biology courses too) as a university professor in Canada (in French at Université de Moncton) and statistics and programming courses overseas (in French at the Université nationale du Rwanda in central Africa).

In 1979, he joined a compiler team for a new 4GL and RDBMS in the US and wrote the parser in DTSS BASIC and code generator (DTSS COBOL) for a set of statistical functions in the compiler, as well as being responsible for system testing and documentation.

In 1980 he joined Hewlett-Packard Canada in 1980 as an operating-systems-internals and database-performance specialist. He won the *Systems Engineer of the Year* Award in 1982. His teaching for HP was primarily on the MPE/3000 operating system internals, IMAGE/3000 database and VPLUS/3000 GUI-design courses. He served as support engineer mostly to HP's hospital and university customers in Montreal and Ottawa; he also managed HP's bilingual call center *(Phone-In Consulting Service)* for Québec & the Maritime provinces from 1981 through 1983.

From 1984 through June 1986 he was Director of Technical Services for MATHEMA Inc., a major service bureau in Montréal at the time. He was responsible for training and supervision of all operations in the 24x365 HP3000-based computing center.

He founded his consulting firm, JINBU Corporation in July 1986 and continued his work as an operations-management consultant, although information security became an ever-important component of his work starting around 1988. He worked extensively on performance optimization for HP computers in several departments of the Canadian government.

He served as Director of Education for the National Computer Security Association (NCSA, later ICSA and then TruSecure and now Verizon's Business Security Solutions) from 1991 to 1999 and then worked with the short-lived AtomicTangerine company, where he supported the *International Institute for Information Integrity*® (I-4®).

He collaborated in the (ISC)² committees defining the *Common Body of Knowledge* for the *Certified Information Systems Security Professional* (CISSP) designation in the mid-1990s and earned his CISSP in 1997 and his ISSMP (*Information Systems Security Management Professional*) in 2005.

Since 1986 (and as of the end of 2016), he has published over 1,300 articles in operations management and security, written a college textbook on enterprise security (McGraw-Hill, 1996), and served as Technical Editor of the 4th (2002), 5th (2009) and 6th (2014) editions of the *Computer Security Handbook* (Wiley). He wrote two security-management columns a week distributed by *Network World* from February 2000 to September 2011 and published one a week in the *InfoSec Perception* blog from October 2011 through November 2013.

He has been an invited lecturer at the United States War College, the Pentagon, NATO HQ in Brussels, and at NATO Counterintelligence training in Germany. He was inducted into the Information Systems Security Association (ISSA) *Hall of Fame* in December 2004.

From January 2002 to June 2009, he was the creator and Director of the *Master's Program in Information Assurance* (MSIA, now MISA) in the School (now College) of Graduate and Continuing Studies (SGCS) at Norwich University, Northfield, Vermont where he was also the Chief Technical Officer of the SGCS from 2007 to 2009.

From July 2001 to April 2011, Dr Kabay was Associate Professor of Computer Information Systems in the School of Business and Management; he became Professor of Computer Information Systems in May 2011. He was appointed Associate Director of the *Norwich University Center for Advanced Computing and Digital Forensics* in July 2011.

Dr Kabay also serves as Strategic Advisor, Information Assurance for a high-tech company, *On Point Cyber* < http://www.opcyber.com/#!team/cjg9 >. His LinkedIn page is < http://www.linkedin.com/mkabay/ > and his Website is < http://www.mekabay.com >.

Students are welcome to *friend* him on Facebook (but to protect their privacy he generally does not follow students) for a stream of links to interesting information security and high-technology articles (mostly from *The Guardian, BBC News* and *National Public Radio*) with occasional forays into politics (especially commie-pinko-radical commentary), culture, science, funny cartoons, pictures of cute animals, and horrible puns.