UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Department of Computer Science

Topics in Advanced Computer Science - Advanced Network Security (CS 789)

Instructor:
Phone:
Office:
Email:
Office hours:
Class website:
Teaching Assistant:

References

1. "Data Mining with Rattle and R", Graham Williams, Springer, 2011, ISBN 978-1-4419-9889-7
2. "BackTrack 5 Wireless Penetration Testing Beginner's Guide", Vivek Ramachandran, 2011, Packet Publishing, ISBN 978-1-849515-58-0
3. "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Syngress, 2011, ISBN-10: 1597496456

Prerequisites

- Any of CS443, CS445, CS448 or equivalent
- CS465 or equivalent

Course description

The purpose of this class is exploring advanced topics in cyber security and developing research capability as graduate students. It will cover the topics in cybersecurity data analytics, wireless security, SCADA security. Students will choose their own topic on cybersecurity research, conduct research, and present it at the end of the semester. Various labs will be introduced to build hands-on skills on network protocols and security. Due to the need for frequent hands-on practice, the course will be held at the Computer Security Lab (WHI 302). Students are encouraged to bring their own laptop computers. Students may stay in the lab after the class to complete labs or assignments if there is no subsequent class.

Student learning outcome

Upon successful completion of this course, students will be able to:

- Analyze the security vulnerabilities in various Internet protocols and study the common threats from the Internet (e.g., DNS cache poisoning, session hijacking, denial-of-service, worm)
- Assess and fix the common security problems in their own computing environment (e.g., use of WPA to avoid wireless packet sniffing)
- Understand the internal mechanisms of the secure Internet protocols both in wired and wireless environment
- Understand common attack methods from the Internet, and have an experience in using software and hardware devices for protection from the attacks
- Understand the software and hardware devices to thwart the attacks from the Internet as well as their operating principles (e.g. Firewall, IDS)

Topics to be covered

- Review of Computer Networks and Cryptography
- Cybersecurity data analytics

    - Big data tools (R/Rattle)
    - Clustering and pattern discovery
    - Association rule analysis
    - Unstructured data mining
- Wireless network security
    - Types of wireless systems and standards
    - WEP Vulnerabilities
    - War driving
    - Attacks on wireless protocols
- Security testing tools and practices
    - Abusing DNS, SNMP
    - Network recon
    - Service identification
    - Breaking windows/Linux passwords
    - Vulnerability scanning
    - Exploiting windows vulnerabilities
    - Intrusion detection with Snort
    - Web hacking with WebGoat
- SCADA Security
    - Architecture of SCADA systems and components in SCADA
    - Industrial network protocols (Modbus, ICCP, DNP3, OLE)
    - Vulnerability in SCADA protocols
    - SCADA Simulation software tools

Assignments

- 2 to 3 assignments
- All assignments should be submitted at the beginning of the class on the due date. No late assignments accepted. (Exceptions: car accident, emergency medical attention, etc., with a proof in writing)
- **No email submissions or WebCapmus submission are accepted (Must be on paper)**
- Scores will be posted on the WebCampus

Quizzes

- 3 to 5 announced quizzes
- No make-up chance for missed quiz
- Scores will be posted on the WebCampus

Student research project

- Individual research report and presentation
- Students will choose independent topic. The topics will be discussed in the class.
- Students submit a research report, and give an 18-minute presentation.
- The presentation content will be included in the final exam

Exams

- Closed books and notes. Multiple choice + short answers
- **NO make-up exams, NO early exams**
- Midterm: Oct. 14, Tuesday
- Final: Dec. 9, Tuesday, 1:00pm – 3:00pm (Range: after midterm)

Evaluation

Area	Weight
Midterm Exam	25%

Final exam		25%
Lab		10%
Quiz		5%
Assignment		10%
Research project	Proposal	5%
	Report	10%
	Presentation	10%

Grading

- Curved (***Rough*** distribution of grades: A: 30%, B: 40%, C or below: 30%)

Tentative Schedule

		Tuesday	Thursday
1	**26-Aug**	Introduction / Internet security review	Cryptography review
2	**2-Sep**	Cybersecurity data analytics	Cybersecurity data analytics
3	**9-Sep**	Project topic selection and research planning	Attending expo (assignments)
4	**16-Sep**	Visiting ORNL (assignments)	Cybersecurity data analytics
5	**23-Sep**	Wireless security	Wireless security
6	**30-Sep**	Wireless security	Wireless security
7	**7-Oct**	Proposal (14 students)	Proposal (5) /Midterm Review
8	**14-Oct**	Midterm exam (25%)	Cybersecurity tools and practice
9	**21-Oct**	Cybersecurity tools and practice	Cybersecurity tools and practice
10	**28-Oct**	Cybersecurity tools and practice	Cybersecurity tools and practice
11	**4-Nov**	SCADA security	SCADA security
12	**11-Nov**	Veterans day Recess - No class	SCADA security
13	**18-Nov**	Presentation (4 students)	Presentation (4)
14	**25-Nov**	Presentation (4)	Thanksgiving day - no class
15	**2-Dec**	Presentation (4)	Presentation (3) / Final exam review
16	**9-Dec**	Final exam (25%)	

Remedial class

- Review class for those who have not taken any kind of cybersecurity classes before.
- **Aug. 29, Friday 2:00pm – 4:00pm, at WHI 302**

Selected UNLV Policies:

Academic Misconduct—Academic integrity is a legitimate concern for every member of the campus community; all share in upholding the fundamental values of honesty, trust, respect, fairness, responsibility and professionalism. By choosing to join the UNLV community, students accept the expectations of the Student Academic Misconduct Policy and are encouraged when faced with choices to always take the ethical path. Students enrolling in UNLV assume the obligation to conduct themselves in a manner compatible with UNLV's function as an educational institution. An example of academic misconduct is plagiarism. Plagiarism is using the words or ideas of another, from the Internet or any source, without proper citation of the sources. See the *Student Academic Misconduct Policy* (approved December 9, 2005) located at: https://www.unlv.edu/studentconduct/student-conduct.

Copyright—The University requires all members of the University Community to familiarize themselves **with** and to follow copyright and fair use requirements. **You are individually and solely responsible for violations of copyright and fair use laws. The university will neither protect nor defend you nor assume any responsibility for employee or student violations of fair use laws.** Violations of copyright laws could subject you to federal and state civil penalties and criminal liability, as well as disciplinary action under University policies. Additional information can be found at: http://www.unlv.edu/provost/copyright.

Disability Resource Center (DRC)—The UNLV Disability Resource Center (SSC-A 143, http://drc.unlv.edu/, 702-895-0866) provides resources for students with disabilities. If you feel that you have a disability, please make an appointment with a Disabilities Specialist at the DRC to discuss what options may be available to you. If you are registered with the UNLV Disability Resource Center, bring your Academic Accommodation Plan from the DRC to the instructor during office hours so that you may work together to develop strategies for implementing the accommodations to meet both your needs and the requirements of the course. Any information you provide is private and will be treated as such. To maintain the confidentiality of your request, please do not approach the instructor in front of others to discuss your accommodation needs.

Religious Holidays Policy—Any student missing class quizzes, examinations, or any other class or lab work because of observance of religious holidays shall be given an opportunity during that semester to make up missed work. The make-up will apply to the religious holiday absence only. It shall be the responsibility of the student to notify the instructor **within the first 14 calendar days of the course for fall and spring courses (excepting modular courses), or within the first 7 calendar days of the course for summer and modular courses,** of his or her intention to participate in religious holidays which do not fall on state holidays or periods of class recess. For additional information, please visit: http://catalog.unlv.edu/content.php?catoid=6&navoid=531.

Transparency in Learning and Teaching
The University encourages application of the transparency method of constructing assignments for student success. Please see these two links for further information:

https://www.unlv.edu/provost/teachingandlearning

https://www.unlv.edu/provost/transparency

Incomplete Grades—The grade of I—Incomplete—can be granted when a student has satisfactorily completed three-fourths of course work for that semester/session but for reason(s) beyond the student's control, and acceptable to the instructor, cannot complete the last part of the course, and the instructor believes that the student can finish the course without repeating it. The incomplete work must be made up before the end of the following regular semester for undergraduate courses. Graduate students receiving "I" grades in 500-, 600-, or 700-level courses have up to one calendar year to complete the work, at the discretion of the instructor. If course requirements are not completed within the time indicated, a grade of F

will be recorded and the GPA will be adjusted accordingly. Students who are fulfilling an Incomplete do not register for the course but make individual arrangements with the instructor who assigned the I grade.

Tutoring and Coaching—The Academic Success Center (ASC) provides tutoring, academic success coaching and other academic assistance for all UNLV undergraduate students. For information regarding tutoring subjects, tutoring times, and other ASC programs and services, visit http://www.unlv.edu/asc or call 702-895-3177. The ASC building is located across from the Student Services Complex (SSC). Academic success coaching is located on the second floor of the SSC (ASC Coaching Spot). Drop-in tutoring is located on the second floor of the Lied Library and College of Engineering TEB second floor.

UNLV Writing Center—One-on-one or small group assistance with writing is available free of charge to UNLV students at the Writing Center, located in CDC-3-301. Although walk-in consultations are sometimes available, students with appointments will receive priority assistance. Appointments may be made in person or by calling 702-895-3908. The student's Rebel ID Card, a copy of the assignment (if possible), and two copies of any writing to be reviewed are requested for the consultation. More information can be found at: http://writingcenter.unlv.edu/.

Rebelmail—By policy, faculty and staff should e-mail students' Rebelmail accounts only. Rebelmail is UNLV's official e-mail system for students. It is one of the primary ways students receive official university communication such as information about deadlines, major campus events, and announcements. All UNLV students receive a Rebelmail account after they have been admitted to the university. Students' e-mail prefixes are listed on class rosters. The suffix is always @unlv.nevada.edu. **Emailing within WebCampus is acceptable.**

Final Examinations—The University requires that final exams given at the end of a course occur at the time and on the day specified in the final exam schedule. See the schedule at: http://www.unlv.edu/registrar/calendars.