

Spring 2020

CS 646-852: Network Protocols Security

Kurt Rohloff

Follow this and additional works at: <https://digitalcommons.njit.edu/cs-syllabi>

Recommended Citation

Rohloff, Kurt, "CS 646-852: Network Protocols Security" (2020). *Computer Science Syllabi*. 76.
<https://digitalcommons.njit.edu/cs-syllabi/76>

This Syllabus is brought to you for free and open access by the NJIT Syllabi at Digital Commons @ NJIT. It has been accepted for inclusion in Computer Science Syllabi by an authorized administrator of Digital Commons @ NJIT. For more information, please contact digitalcommons@njit.edu.

COURSE SYLLABUS

CS 646

Network Protocols Security

Spring 2020

Instructor: Kurt Rohloff

Credits:	3
Section:	852
Class hours:	Online
Lecture Location:	Online
Course Website:	moodle

Instructor Info:

Instructor Office:	GITC (Computer Science Building)
Instructor Office Hours:	In person: By appointment Online: Thursday 9pm-10pm
Instructor E-mail:	rohloff@njit.edu

Grader Info:

We will have a grader, but this person will be working behind the scenes.

1 DESCRIPTION

The course focuses on the security of network protocols. The goal of the course is to familiarize students with common threats and attacks, and to study the fundamental techniques used to secure network communication over insecure channels. The course will have an applied component, which will help students gain practical experience in attacking and defending networked systems. Topics include authentication systems, secure communication at data link, network, transport and application layers, vulnerabilities of Internet protocols, DNS and routing security, firewalls, intrusion detection, honeypots, wireless networks security, malware propagation and detection, and web security.

2 ORGANIZATION

This is a lecture course with an extensive self-learning experiential component during outside projects and homework. Topics are introduced and presented by the instructor, with a focus on big-picture concepts and practical implications. Student participation through forum discussion is encouraged.

Students are assigned homework focused on topics discussed in lecture. There will be assigned readings from supplementary materials. The initial lectures are structured and scheduled, but we leave flexibility in the schedule to discuss topics of current interest selected with input from students. There will be a mid-term, a final exam and a course project.

3 COURSE OBJECTIVES

At the end of the course, students are expected to have an understanding of:

1. Review of computer networking fundamentals
2. Common vulnerabilities and attacks, including malware and Advanced Persistent Threats
3. Firewalls, Tor and other Circumvention Mechanisms
4. Wireless networking & security; DoS attacks against 802.11
5. Practical Cryptography, AES and Friends, Public-key
6. Key Establishment Protocols using symmetric key crypto.
7. Key agreement using public key crypto (Diffie Hellman, STS protocol)
8. Public Key Infrastructure
9. Authentication, Logging In, Kerberos authentication protocol
10. Major networking protocols (DNS, BGP, IPsec, etc...), their vulnerabilities and security features.
11. Identity management techniques and limitations.
12. Access Control (if there is space left)
13. Privacy Protection

4 TEXT AND REQUIRED SUPPLIES

Required text: None

Optional Supplemental Texts:

1. Computer Networking: A Top-Down Approach by Kurose and Ross (any edition, but the later the better.)

Additional easily downloadable material will be assigned over the term

This class and homework will be experiential and experimentally focused. You are expected to have access to machines with Unix/Linux command line with root access, a network and the ability to install software. MacOS **may** be fine, but your mileage may vary. Virtual machines running on a Windows machine are fine. An Amazon cloud server is fine. AFS access should be okay, but mileage may vary.

Be sure to follow all applicable laws and standard rules of good conduct in your locality, when applicable.

5 YOUR IDEAS, EVALUATIONS, ETC.

In general, your ideas, comments, suggestions, questions, grade challenges, etc. are welcome. Your discretion in these matters is expected, however. No part of your grade will be based on anything other than your assignments.

You are encouraged to take advantage of instructor office hours for help with coursework or any other subject connected with the course and your progress.

6 GRADING PLAN

Final grades are weighted as follows:

- | | |
|-------------------|-----|
| 1. Homework: | 20% |
| 2. Mid-term Exam: | 35% |
| 3. Final Exam: | 45% |

Any violations of the honor code, including plagiarism, copying, mis-representing others' work, or mis-representing your own work will be treated severely, including referral to the Dean of Students.

Please submit all homework and project work through the course moodle site. I am generally lenient about turning in homework late, as long as homework is submitted before course staff begins to grade them.

Homework not turned in by the time the grader begins work will be considered late and homework will be then be marked as 0%.

Any grading, exam or homework policies which are in violation of standard operating procedure at NJIT will be corrected to conform to NJIT policy. All times are Eastern.

7 SUGGESTIONS FOR SUCCESS

For most students this course will at times be “challenging”, and at times “easy”. However, independent, big-picture thinking is most important to your success. Please challenge yourself and your classmates to see the forest from the trees.

