CIS/CSE 644: Internet Security

Description

Topics covered in this course:

- Internet architecture
- Security and attacks on TCP/IP, DNS, and BGP protocols
- Internet protocol security
- Firewall
- Intrusion detection
- Network traceback
- Encryption
- Public-key infrastructure
- One-way hash function
- Digital signature
- Security protocols

Credits

3

Learning Objectives

After taking this course, students will be able to

- explain how the Internet works
- evaluate the risks faced by the Internet and networked computer systems
- explain how various network-based attacks work
- gain first-hand experience with common attacks on the Internet
- use cryptography, including secret-key encryption, one-way hash, and public-key encryption, to secure network communications
- use security technologies, such as firewall and VPN, to protect networks
- design and implement basic security mechanisms to protect against network attacks.

Bibliography/Texts/Supplies Required

- Du, Wenliang. *Internet Security: A Hands-on Approach*. CreateSpace Independent Publishing Platform. ISBN-10: 154836794X, ISBN-13: 9781548367947.

Lab Environment

- There is no need for a physical lab space.

- All the lab activities can be carried out on students' computers.
- Virtual Machine (VM) images are provided, and all the labs have been tested in the images.
- All software used in the lab environment is open source and free.

Grading

Participation: 10% (the grade will be based on students' participation in the synchronous sessions and the submission of the lecture exercises while watching the lectures)(30/100 for lecture exercise, due by live session. No regrading afterward, 70/100 for live session participation)

Final exam: 40% (there will be a proctored exam during the synchronous session in week 11).

- Since the exam is online, being late to the final exam means a student with the exam, which is posted 10 minutes before the exam starts, is not being proctored during that period of time, and will be considered as a violation of the proctoring rule. We therefore deduct 2-3 point for each late minute. For example, if a student is late for 10 minutes, 20-30 points will be deducted from the exam.
- During the exam, students cannot use computers. Students are required to print out the exam questions on paper; they cannot look at the exam from the computer monitor. Students who keep watching the computer screen is considered as cheating, and will receive 0 for the exam. Students are allowed to occasionally look at their monitors to see whether the professor has made any online announcement.
- Camera should be setup in a way for the professor to view the whole table, the scanner and printer. If student has to leave for the scan, please show each answer page to the camera first. The final will be recorded.

Labs: 43% (please see the Lab Report Requirements document for more details)

Lab	Weight in final grade
Lab 1	7%
Lab 2	7%
Lab 3	7%
Lab 4	4%
Lab 5	4%
Lab 6	5%
Lab 7	9%
Total	**43%**

Quiz: 7%

Quiz	Weight in final grade
Quiz 1a	0.5%
Quiz 1b	0.5%
Quiz 2	1%
Quiz 3	1%
Quiz 4	1%
Quiz 5	1%
Quiz 6	1%
Quiz 7	1%
Total	**7%**

The final grade will be based on the following criterion:

90–100	A
85–89	A-
80–84	B+
75–79	B
70–74	B-
65–69	C+
60–64	C
50–59	C-
< 50	F

Course Specific Policies on attendance, late work, make-up work, examinations if outside normal class time, etc.

A deduction will be applied to late homework submission. 10% will be deducted per business day, excluding weekends and holidays.

Academic Integrity Policy

Syracuse University's academic integrity policy reflects the high value that we, as a university community, place on honesty in academic work. The policy defines our expectations for academic honesty and holds students accountable for the

integrity of all work they submit. Students should understand that it is their responsibility to learn about course-specific expectations, as well as about university-wide academic integrity expectations. The university policy governs appropriate citation and use of sources, the integrity of work submitted in exams and assignments, and the veracity of signatures on attendance sheets and other verification of participation in class activities. The policy also prohibits students from submitting the same written work in more than one class without receiving written authorization in advance from both instructors. The presumptive penalty for a first instance of academic dishonesty by an undergraduate student is course failure, accompanied by a transcript notation indicating that the failure resulted from a violation of academic integrity policy. The presumptive penalty for a first instance of academic dishonesty by a graduate student is suspension or expulsion. SU students are required to read an online summary of the university's academic integrity expectations and provide an electronic signature agreeing to abide by them twice a year during preterm check-in on MySlice. For more information and the complete policy, see http://academicintegrity.syr.edu/.

Disability-Related Accommodations

If you believe that you need accommodations for a disability, please contact the Office of Disability Services (ODS), http://disabilityservices.syr.edu/, located in Room 309 of 804 University Avenue, or call (315) 443-4498, TDD: (315) 4431371 for an appointment to discuss your needs and the process for requesting accommodations. ODS is responsible for coordinating disability-related accommodations and will issue students with documented Disabilities Accommodation Authorization Letters, as appropriate. Since accommodations may require early planning and generally are not provided retroactively, please contact ODS as soon as possible.

Syracuse University values diversity and inclusion; we are committed to a climate of mutual respect and full participation. My goal is to create learning environments that are usable, equitable, inclusive, and welcoming. If there are aspects of the instruction or design of this course that result in barriers to your inclusion or accurate assessment or achievement, I invite any student to meet with me to discuss additional strategies beyond accommodations that may be helpful to your success.

Religious Observances Notification and Policy SU religious observances notification and policy, found at http://hendricks.syr.edu/spiritual-life/index.html, recognizes the diversity of faiths represented among the campus community and protects the rights of students, faculty, and staff to observe religious holidays according to their tradition. Under the policy, students are provided an opportunity to make up any examination, study, or work requirements that may be missed due to a religious observance provided they notify their instructors before the end of the second week of classes for regular session classes and by the submission deadline for flexibly formatted classes.

For fall and spring semesters, an online notification process is available for students in **My Slice / StudentServices / Enrollment / MyReligiousObservances / Add a Notification**. Instructors may access a list of their students who have submitted a notification in My Slice Faculty Center.

Student Academic Work Policy

SU policy on student academic work may be found at: http://coursecatalog.syr.edu/content.php?catoid=3&navoid=270#Student_Academic_Work

Student work prepared for University courses in any media may be used for educational purposes, if the course syllabus makes clear that such use may occur. You grant permission to have your work used in this manner by registering for, and by continuing to be enrolled in, courses where such use of student work is announced in the course syllabus.

Course Schedule

Week	Session/Unit	Assignments
1	Introduction and overview of the TCP/IP protocols	Lab setup
2	Sniffing and Spoofing	Lab 1 (Sniffing and Spoofing) Quiz 1a is due at the end of this live session.
3	IP and ICMP protocols, and attacks on them	Lab 1 continuation Lab 1 report must be submitted before 11:59pm one day before live session 4. Quiz 1b is due at the end of this live session.
4	Firewall	Lab 2 (Firewall) Lab 2 report must be submitted before 11:59pm one day before live session 5. Quiz 2 is due at the end of this live session.
5	UDP and TCP protocols, and attacks on UDP and TCP	Lab 3 (TCP attacks) Lab 3 report must be submitted before 11:59pm one day before live session 6. Quiz 3 is due at the end of this live session.
6	DNS protocol and attacks	Lab 4 (DNS attacks) Lab 4 report must be submitted before 11:59pm one day before live session 7. Quiz 4 is due at the end of this live session.

7	Secret key encryption and oneway hash function	Lab 5 (Encryption) Lab 5 report must be submitted before 11:59pm one day before live session 8. Quiz 5 is due at the end of this live session.
8	Public key encryption	Lab 6 (PKI) Lab 6 report must be submitted before 11:59pm one day before live session 9. Quiz 6 is due at the end of this live session.
9	Virtual Private Network	Lab 7 (VPN) Quiz 7 is due at the end of this live session.
		Lab 7 is due one day before live session
10	BGP protocol	No assignment
11	Final exam	Proctored final exam during live session 11

Weekly Reading Assignments

Note: Additional readings will be posted on the course wall.

Week	*Readings*
1	**RECOMMENDED READING** *Wikipedia*. "Address Resolution Protocol." Last modified December 2, 2016, https://en.wikipedia.org/wiki/Address_Resolution_Protocol.
2	**REQUIRED READING** Chapter 12. *Computer Security: A Hands-on Approach by W. Du*

3	**RECOMMENDED READING** *Wikipedia.* "Internet Control Message Protocol." Last modified November 27, 2016, https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol. *Wikipedia.* "Internet Protocol." Last modified November 25, 2016, https://en.wikipedia.org/wiki/Internet_Protocol. Ziemba, G. Paul, Darren Reed, and Paul Traina. "RFC 1858 - Security Considerations for IP Fragment Filtering." *Faqs.* October 1995. Accessed December 6, 2016, http://www.faqs.org/rfcs/rfc1858.html.
4	**REQUIRED READING** Chapter 14. *Computer Security: A Hands-on Approach by W. Du*
5	**REQUIRED READING** Chapter 13. *Computer Security: A Hands-on Approach by W. Du*
6	**REQUIRED READING** Chapter 15. *Computer Security: A Hands-on Approach by W. Du*

RECOMMENDED READING Schneider, David. "Fresh Phish." *IEEE Spectrum: Technology, Engineering, and Science News*, 2008. Accessed December 06, 2016.

7 **REQUIRED READING**

Wikipedia. "Block Cipher Mode of Operation." Last modified November 30, 2016, https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation.
Du, Wenliang. Lecture notes. PDF. Syracuse University.
Freidl, Steve. "An Illustrated Guide to Cryptographic Hashes." *Steve Friedl's Unixwiz.net Tech Tips.* Last modified May 9, 2005, http://www.unixwiz.net/techtips/iguide-crypto-hashes.html.

RECOMMENDED READING

Wikipedia. "Advanced Encryption Standard." Last modified November 26, 2016, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
Kohno et al. "Analysis of an Electronic Voting System." PDF. *IEEE*, 2004.
Markoff, John. "Flaw Found in an Online Encryption Method." *New York Times*, February 14, 2012. Accessed December 07, 2016, http://www.nytimes.com/2012/02/15/technology/researchers-find-flawin-an-online-encryption-method.html?pagewanted=1&ref=johnmarkoff.
Defuse. "Encryption - CBC Mode IV: Secret or Not?" September 8, 2013. Accessed December 07, 2016, https://defuse.ca/cbcmodeiv.htm.

8 **REQUIRED READING**

Chapters 18 and 19. *Computer Security: A Hands-on Approach by W. Du*

Du, Wenliang. Lecture notes. PDF. Syracuse University.

RECOMMENDED READING

Wikipedia. "Public Key Cryptography." Last modified December 5, 2016,https://en.wikipedia.org/wiki/Public-key_cryptography.
Wikipedia. "RSA." Last modified November 27, 2016, https://en.wikipedia.org/wiki/RSA_(cryptosystem).
Wikipedia. "Transport Layer Security." Last modified December 5, 2016, https://en.wikipedia.org/wiki/Transport_Layer_Security.

9 **REQUIRED READING**

Chapter 16. *Computer Security: A Hands-on Approach by W. Du*

RECOMMENDED READING

Friedl, Steve. "An Illustrated Guide to IPsec." *Steve Friedl's Unixwiz.net Tech Tips.* August 24, 2005. Accessed December 07, 2016, http://www.unixwiz.net/techtips/iguide-ipsec.html.

Wikipedia. "OpenVPN." Last modified November 26, 2016, https://en.wikipedia.org/wiki/OpenVPN.

Wikipedia. "Virtual Private Network." Last modified November 28, 2016,https://en.wikipedia.org/wiki/Virtual_private_network.

10 **REQUIRED READING**

Butler et al. A Survey of BGP Security. PDF. *Patrickmcdaniel.org.* April, 2005.

RECOMMENDED READING

Ripe NCC. "BGP Routing information about Syracuse University (AS11872)." Accessed December 7, 2016, https://stat.ripe.net/as11872#tabId=at-aglance.

Wikipedia. "Border Gateway Patrol." Last modified December 7, 2016, https://en.wikipedia.org/wiki/Border_Gateway_Protocol.

Nordstöm, Ola, and Constantinos Dovrolis. Beware of BGP Attacks. PDF. Georgia Institute of Technology.

Ripe NCC. "Routing Information Service." Last modified September 30, 2016, https://www.ripe.net/analyse/internet-measurements/routinginformation-service-ris/routing-information-service-ris.