UNIVERSITY of VIRGINIA | SCHOOL of ENGINEERING & APPLIED SCIENCE
Department of Computer Science

CS 4501 - 003: Network Security

Fall 2017 Syllabus

Instructor: Ahmed Ibrahim / Rice Hall 207 / a.i@virginia.edu / (434) 924-8284
Lecture Location: Rice Hall, Room 130
Lecture Time: Weekly on Monday & Wednesday 3:30pm-4:45pm
Office Hours: Mon 5:00pm-6:30pm / Wed 2:00pm-3:00pm & by appointment (in Rice Hall 207)

1 Who should take this course (aka Prerequisites)

I expect that you have no prior knowledge about the topics discussed in this class. Enthusiasm is a must though! You must have passed CS 2150 with a grade of `C-` or better and be able to develop/interpret programs.

2 A bit about the course (aka Course Description)

This course covers the principles of secure network communications and the application of network security. Topics include: attack types, attack surfaces, attack phases, network security devices, (a)symmetric key encryption, cryptographic hash function, authentication/identification techniques, key distribution, and data integrity assurance. Also, currently used security mechanisms and protocols such as WEP, Kerberos, X.509 certificates, PKI, SSL/TLS, IPsec, S/MIME, PGP, and VPN will be discussed.

3 What you'll learn along the way (aka Course Objectives)

The overriding goal for the course is for you to begin thinking critically about how security services are designed. In this course, you will learn the principles of secure network communications and the application of network security without the need or desire to delve deeply into cryptographic theory and principles. Is there a one-size-fits-all security mechanism? Shall we think of security as a core element of the system design process, or as an element that needs to be incorporated after the system design is complete? While you are answering those type of questions, you will be able to:

1. Identify types of cyber attacks and attacks' phases
2. Describe and differentiate between the main network security services
3. Evaluate, compare, and contrast symmetric and asymmetric encryption
4. Combine symmetric and asymmetric encryption to offer an affordable secure way of communication
5. Describe the basic structure and usage of network security mechanisms
6. Research a security concept, mechanism, or protocol
7. Explain a security mechanism (or protocol) to someone who is not an expert in this field.

4 Where's the material coming from (aka Textbook)

Material from several sources will be used and presented. However, the majority of the materials is from the ***Network Security Essentials Applications and Standards***, 6^{th} edition, textbook by William Stallings (Pearson, ISBN 9780134527338). The bookstore has the paperback version, the cost is $112.80 for new and $84.60 for used. You do **NOT** have to purchase the textbook. You will be required to perform online exercises from Infosec Learning (http://infoseclearning.com) which cost about $90 - $100 total. There may be other on-line readings. The class meetings schedule will be posted on the course UVaCollab website. You are responsible for checking the UVaCollab website regularly.

5 How you'll learn (aka Assessment)

You will experience a valuable learning experience by attending all class meetings, paying attention, asking questions, and actively participating in discussions.

QUIZZES

Unannounced quizzes will be given at the beginning of some lectures to reinforce the basics. Quizzes will be in the form of multiple choice questions, true/false, or short answer. If you miss a quiz (or two) due to an acceptable excuse, you can make it up - within a reasonable time frame - as long as you don't know the questions on that quiz.

HOMEWORKS

Regular homeworks will be announced on the course's UVaCollab website. Homeworks will be in formats (multiple choice questions, true/false, short answer, understanding a program, writing a program, etc) which help you review and practice what you have learned. Homeworks also allow you to demonstrate your understanding of the course elements. All homeworks are individual work. Each homework will include a due date, a late submission policy (if applicable), and a regrade policy.

TEAM PROJECT

You will get to contribute to a semester-long team project. This project will encourage you to ask some big questions about how a security mechanism or protocol works and why/when to use it. You will demonstrate your understanding through activities such as creating a plan that includes the answers for your big questions and producing a video which explains your topic of interest to someone who is not an expert in this field. You will be able to choose from a set of topics or propose your own topic. Details will be discussed at the beginning of the course.

EXAMS

You will have two exams in this course, a midterm exam and a final exam. The midterm exam is closed-book closed-notes and covers the topics you experienced in the first half of this course. The final exam (Friday, December 15, 2017 1400-1700) is closed-book closed-notes and covers ALL the topics you experienced in this course.

6 How you will earn your grade (aka Evaluation)

The grade you will earn for this course will be based on how well you demonstrate your learning using the following ways:

Quizzes & Homeworks	**25%**	Composed of unannounced quizzes and regular announced homeworks
Team Project	**25%**	Phase 1 due 9/22 – Phase 2 due 10/31 – Phase 3 due 11/21
Midterm Exam	**25%**	Wednesday, October 11, 2017 (closed-book closed-notes) Covers all the topics you learned until the exam
Final Exam	**25%**	Friday, December 15, 2017 (closed-book closed-notes) Covers all the topics you learned until the exam

Your overall score will be mapped to a letter grade as follows:

A+	100	98.000	C+	79.999	77.000
A	97.999	93.000	C	76.999	73.000
A-	92.999	90.000	C-	72.999	70.000
B+	89.999	87.000	D+	69.999	67.000
B	86.999	83.000	D	66.999	63.000
B-	82.999	80.000	D-	62.999	60.000

Any score below 60 will be mapped to a **F** letter grade. By default, grades will not be rounded in this course.

7 Stops Along the Way (aka Tentative Schedule)

The following times and topics are tentative and may shift slightly to foster a more effective learning environment. Nothing will be made due earlier than indicated but some things may be pushed back or eliminated altogether, depending on time.

Week	Date	Chapter	Topic
1	Wed. Aug 23	-	Course Introduction and Scope
2	Mon. Aug 28	-	Team Project Discussion and Project Assignments
	Wed. Aug 30	1 & 11.3	Physical Attacks, Software Attacks, and Password Cracking
3	Mon. Sep 4	1 & 10	Malware, Web-App Based Attacks, and Social Engineering Attacks
	Wed. Sep 6	1	Threat Modeling, Security Services, Incident Res., and Attack Phases
4	Mon. Sep 11	-	Pen Testing, Red/Blue Teams, Threat Hunting, Traffic Analysis
	Wed. Sep 13	-	Network Forensics and Traffic Analysis
5	Mon. Sep 18	12	Network Security Devices and Security Design Principles
	Wed. Sep 20	2	Symmetric Encryption Principles **PHASE 1 DUE 9/22**
6	Mon. Sep 25	2 & 7	Stream Ciphers, One-Time Pad, RC4, and WEP
	Wed. Sep 27	2	Block Ciphers, Fiestel Structure, DES (and S-DES)
7	Mon. Oct 2	-	READING DAY (No Class Meeting)
	Wed. Oct 4	2	2DES, 3DES, AES, and Modes of Operation
8	Mon. Oct 9	-	Review
	Wed. Oct 11	-	**MIDTERM EXAM**
9	Mon. Oct 16	3	MACs and Hash Functions (MD5 + SHA-family)
	Wed. Oct 18	3 & 4	Kerberos and Asymmetric Encryption Principles
10	Mon. Oct 23	4	Asymmetric Key Distribution and User Authentication
	Wed. Oct 25	-	Project Discussion
11	Mon. Oct 30	4	Chain of Trust / Digital Signatures / X.509 DCs **PHASE 2 DUE 10/31**
	Wed. Nov 1	4	Public Key Infrastructure and Key Management
12	Mon. Nov 6	6	Transport Layer Security (SSL/TLS)
	Wed. Nov 8	6	SSL/TLS Attacks - Heartbleed / MITM / SSLStrip / SSLSniff / ...
13	Mon. Nov 13	8	DNS Attacks and DNSSEC - DNS Spoofing Activity
	Wed. Nov 15	-	Project Discussion
14	Mon. Nov 20	8	E-mail Security (S/MIME & PGP) **PHASE 3 DUE 11/21**
	Wed. Nov 22	-	HAPPY THANKSGIVING (No Class Meeting)
15	Mon. Nov 27	9	IP Security
	Wed. Nov 29	-	Select Topic/Presentation or Guest Lecture
16	Mon. Dec 4	-	Review

8 When you need help (aka Communication)

Do not hesitate to contact me if you have any problems, concerns, questions, or issues regarding the course, material, or anything else in the class. We (faculty) in general have an "open door" policy, in that if our door is open, by all means stop on in and say "hi" or ask a question. If our doors are closed, then we're working on some task, on the phone, in a meeting, etc. It is always a good idea to e-mail or call before coming to make sure we are here if it is *not* office hours.

We will use **Piazza** for class discussion. The system is highly catered to getting you help fast and efficiently from classmates, TAs, and professors. Rather than e-mailing me course-oriented questions, please post them on Piazza. You can also make posts just to the instructors and TAs, or you can direct it to a single person. In case it is a personal issue, e-mail me directly.

If you would like to e-mail me, don't just reply to an e-mail which I have sent earlier as the subject will not match the purpose of your e-mail. That makes it harder on me to keep up with your e-mail. Always remember to use a meaningful subject and put **"CS 4501"** somewhere in the subject in order to make it easier on me. Thank you!

9 SDAC and Other Special Circumstances

If you have been identified as an SDAC student, please let the Student Disability Access Center know you are taking this class. If you suspect you should be an SDAC student, please schedule an appointment with them for an evaluation. We happily and discretely provide the recommended accommodations for those students identified by the SDAC. Please contact us one week before an exam so we can make accommodations. Website: `http://www.virginia.edu/studenthealth/sdac/sdac.html`

If you have other special circumstances (athletics, other university-related activities, etc.) please contact your instructor and/or Head TA as soon as you know these may affect you in class.

10 Research

Your class work might be used for research purposes. For example, I may use anonymized student assignments to design algorithms or build tools to help programmers. Any student who wishes to opt out can contact me to do so after final grades have been issued. This has no impact on your grade in any manner.

11 A few more points (aka Academic Integrity)

In this course, there will be a focus on working well together and learning about the development process. A large portion of that process involves interpersonal skills and conflict management. We are all expected to treat each other with respect.

PROFESSIONALISM PENALTY

Excessive missed classes, rude behavior, unauthorized homework assistance, etc can be held against a student when final grades are calculated (Up to -100%). Note that academic dishonesty infractions can lead to a **F** in the class.

If a student submits a solution that he or she did not author (i.e. copied from another student or from the Internet), or if another student submits code/solution that matches your code/solution, then the student's overall course grade will be dropped significantly.

HONOR POLICY

The School of Engineering and Applied Science relies upon and cherishes its community of trust. We firmly endorse, uphold, and embrace the University's Honor principle that students will not lie, cheat, or steal, nor shall they tolerate those who do. We recognize that even one honor infraction can destroy an exemplary reputation that has taken years to build. Acting in a manner consistent with the principles of honor will benefit every member of the community both while enrolled in the Engineering School and in the future.

Students are expected to be familiar with the university honor code, including the section on academic fraud (`http://www.virginia.edu/honor/what-is-academic-fraud-2/`). Each assignment will describe allowed collaborations, and deviations from these will be considered Honor violations. If you have questions on what is allowable, ask! Unless otherwise noted, exams and individual assignments will be considered pledged that you have neither given nor received help. (Among other things, this means that you are not allowed to describe problems on an exam to a student who has not taken it yet. You are not allowed to show exam papers to another student or view another students exam papers while working on an exam.) Send, receiving or otherwise copying electronic files that are part of course assignments are not allowed collaborations (except for those explicitly allowed in assignment instructions).

Assignments or exams where honor infractions or prohibited collaborations occur will receive a zero grade for that entire assignment or exam. Such infractions will also be submitted to the Honor Committee if that is appropriate. Students who have had prohibited collaborations may not be allowed to work with partners on remaining homeworks.

12 One last point, really (aka Updates)

This syllabus is your guide to this course. In this syllabus, you will find nearly everything you need to know about how the course will be run, what you should expect, and what will be expected of you. However, this syllabus is subject to revisions and updates. You will be notified of any substantial changes or updates. Reasonable notification will be provided to students prior to any major changes. Finally, authority on any decision in this course rests with me, not with this document