JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Syllabus
Computer Science 601.644
Network Security
Fall 2018
(3 credits)

Description

ISIS: This course focuses on communication security in computer systems and networks. The course is intended to provide students with an introduction to the field of network security. The course covers network security services such as authentication and access control, integrity and confidentiality of data, firewalls and related technologies, Web security and privacy. Course work involves implementing various security techniques. A course project is required.

Instructor Comments: This class is focused on network protocols, network architectures, and network utilities. This course is networking and programming intensive. If you do not have a background in these areas, you should NOT take the class

Prerequisites

Recommend Course Background: moderate to advanced computer programming, a basic understanding of TCP/IP network architecture, or permission.

The student registering for this course should be familiar with network protocols and specifically the TCP/IP stack.

Instructor

Professor Seth James Nielson
Email: sethjn@cs.jhu.edu
Office: Malone 303, 410-497-7384
Office hours: MW 1300-1500 and by appointment

Teaching Assistants

Steven Cheng (stevencheng@jhu.edu)
Chanakya Gaur (cgaur1@jhu.edu)

Textbook

Required:

Ross Anderson, *Security Engineering,* http://www.cl.cam.ac.uk/~rja14/book.html

Additionally, there will be many other documents used throughout the semester including RFC's, technical specifications, and contemporary research papers. All of these sources will be available on the Internet; links will be provided in class at the appropriate time.

This class deals lightly with cryptography and mostly in application only. If you have questions about cryptographic primitives or operations, you can consult the "Handbook of Applied Cryptography."

This book is also freely available online.

Online Resources

- Grading: Blackboard
- Discussion: GitHub
- Home Page: GitHub

Course Objectives

(1) Understand basic elements of secure network design
(2) Build prototypical security protocols and applications
(3) Know network security protocols from the lowest layers of the stack up to applications and overlays

Course Topics

- Usable Security Design
- Security Protocols and Access Controls
- Network Attacks/Defense
- ***Network Protocols***

Course Expectations & Grading
This course covers the theory and current practice of network security. Your evaluation will be derived from your ability to apply theory to technology as well as your ability to communicate technical concepts with others.

- Lab Work (50%) – Your lab project is the largest single component of your grade. There are four labs:
    - Transport Layer
    - Secure Transport Layer
    - Network Attack/Defense Project
    - Wargames!

  Labs 2 – 4 are completed as a team.
- Communications (30%) – There are three technical writing assignments. One of the technical writing assignments is submitted individually and is worth 10% of your final grade. The other two writing assignments and are completed as a team and are associated with labs 2, 3. Each of these is worth 5% of your final grade. Additionally, class participation is 10% of your grade.
- Exams (20%) – The mid-term and final exams are worth 10% of your grade each. All the exams require written answers by individual students. Both the mid-term and the final are timed in-class exams.
- There is a programming test on the second class period. Your score will not be technically graded, but it will be used in calculating "bitpoints" (bitpoints may be renamed "galactic credits"). Bitpoints will be used in calculating your grade for the Wargames lab.
- Assigned readings including the book will be evaluated on the exams

A letter grade will be assigned according to this formula:

- 93% and above: **A**
- < 93%: **A-**

- < 90%: **B+**
- < 87%: B
- < 83%: **B-**
- < 80%: **C+**
- < 77%: **C**
- < 73%: **C-**
- < 70%: **D**
- < 60%: **E**

Appropriate curving will be made as necessary

CLASS PARTICIPATION, ATTENDANCE POLICY

New this year, are the following policies:

- You are NOT excused from class for interviews, career fairs, etc. If you miss class, you *will* be penalized. In the case of an excused absence (e.g., confining illness), you must contact me for make-up work.
- Electronics devices may NOT be used in class except for class purposes
- Participation is 10% of your grade. It is your job to make sure I know your name and that I know you are contributing to and participating in the class.
- I will take a roll call each class period and will ask if class readings have been completed. Any day in which you do not have your readings complete will result in a 0 for that day's participation.

Schedule, Assignments, & Readings

NOTE: Readings are due *before* class.

Date – Lecture Title	**Reading/Topics**	**Assignments**
8/30 – Introduction	Introduction part 1.	
9/5 – Assessment		Programming Test in Class
9/10 – Network Background	RFC's OSI Model TCP/IP IPv4 vs IPv6	
9/12 – Security Engineering	Anderson Ch1, Ch2	Transport PRFC DUE
9/17 – Cryptography Review	Anderson Ch3, Ch5 Symmetric primitives Asymmetric primitives Hashing, HMAC, Signatures Certificates. Certificate Chains Hybrid Cryptography	Lab #1: Transport Layer Start
9/19 – Security Objectives	Anderson Ch4 CIA IAAA	
9/24 – Layer 2 Security	Anderson Ch 21 ARP Poisoning Transparent Firewalls	Lab #1 Milestone: Pass through layer with basic encapsulation

9/26 – Layer 3/4 Security	Anderson Ch 21. (pp. 633-642, 652-660, 669-670) Attacks on IP and TCP IP-Sec Firewalls	
10/1 - Layer 3/4 continued	Anderson Ch 21. (pp. 642-643, 675-676) Google Beyond Corp (Zero Trust) DNS, DNSSec VPNs	Lab #1 Milestone: Correct, *interoperable* transmissions when there are no errors
10/3 – Transport Security	Review Anderson Ch 3 Kerberos	
10/8 – Transport Security	Anderson ch 21 (pp.665-666) SSH	Lab #1 Milestone: Correct, *interoperable* transmissions when there are errors
10/10 – Transport Security	Anderson Ch 21 (pp. 670-675) TLS	
10/15 – MIDTERM REVIEW		Lab #1 DUE Intergalactic Game Online Bank Online
10/17 – MIDTERM (In class)		
10/22 – Wireless Security	Anderson Ch 21. (pp. 666-668) WiFi security schemes Bluetooth Cellphone security schemes	Secure Transport PRFC DUE
10/24 – Software Defined Networks		Lab #2 Start
10/29 – Access controls 2	Anderson Ch 8, 9 Bell Lapadula Biba Clark-Wilson MAC v DAC	
10/31 – Web Security	Anderson Ch 23 (pp. 734-739) HTTP HTTPS Cookies XSS CSRF	Lab #2 Milestone: Correct operation without certificate verification
11/5 - Mobile Code		
11/7 – P2P Security, Social Media Security	Anderson Ch 23 (pp. 739-744)	Lab #2 DUE Lab #3 Start Lab #4 Start
11/12 – Passwords, two-factor, SSO		
11/14 – Consensus Protocols,		Lab #3 Milestone: Project

such as Blockchain		approval
11/26 – Banking, Telecommunications, and Medicine	Anderson Ch 10	
11/28 – Physical Protection	Anderson Ch 11, 16 HSMs	
12/3 – Proxies and TOR		
12/5 – Malware	Zero days Metasploit	Lab #3 and #4 DUE!

Ethics

The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful, abiding by the *Computer Science Academic Integrity Policy*:

> Cheating is wrong. Cheating hurts our community by undermining academic integrity, creating mistrust, and fostering unfair competition. The university will punish cheaters with failure on an assignment, failure in a course, permanent transcript notation, suspension, and/or expulsion. Offenses may be reported to medical, law or other professional or graduate schools when a cheater applies.
>
> Violations can include cheating on exams, plagiarism, reuse of assignments without permission, improper use of the Internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition. Ignorance of these rules is not an excuse.
>
> Academic honesty is required in all work you submit to be graded. Except where the instructor specifies group work, you must solve all homework and programming assignments without the help of others. For example, you must not look at anyone else's solutions (including program code) to your homework problems. However, you may discuss assignment specifications (not solutions) with others to be sure you understand what is required by the assignment.
>
> *If* your instructor permits using fragments of source code from outside sources, such as your textbook or on-line resources, you must properly cite the source. Not citing it constitutes plagiarism. Similarly, your group projects must list everyone who participated.
>
> Falsifying program output or results is prohibited.
>
> Your instructor is free to override parts of this policy for particular assignments. To protect yourself: (1) Ask the instructor if you are not sure what is permissible. (2) Seek help from the instructor, TA or CAs, as you are always encouraged to do, rather than from other students. (3) Cite any questionable sources of help you may have received.
>
> On every exam, you will sign the following pledge: "I agree to complete this exam without unauthorized assistance from any person, materials or device. [Signed and dated]". Your course instructors will let you know where to find copies of old exams, if they are available.

In addition, the specific ethics guidelines for this course are:

1. You may not use materials from previous semesters of this course
2. You may work together on the lab work after lab #1, provided you give me a "partnership" agreement.
3. You may not get help from any person, or any Internet source, on the exams

4. Highly ethical behavior is expected when using computing tools and techniques especially when working at on-campus or remote computing facilities.
5. This class, for teaching purposes, requires you to behave in a way that, in almost all other contexts, is unethical and often illegal. You need to understand how the "bad guys" think in order to protect against them. That should in no way encourage you to become one of the "bad guys."
6. Even within this class, you need to recognize the limits of the attacks you can carry out against other students. The whole point of PLAYGROUND is to provide you an opportunity to safely spar with each other. Do not, under any circumstances, try to attack a classmate outside of the PLAYGROUND environment. It is your responsibility to understand what is permissible. If you have any questions, please ask the instructor for guidance.

Report any violations you witness to the instructor.

You can find more information about university misconduct policies on the web at these sites:

- For undergraduates: http://e-catalog.jhu.edu/undergrad-students/student-life-policies/
- For graduate students: http://e-catalog.jhu.edu/grad-students/graduate-specific-policies/

Students with Disabilities
Any student with a disability who may need accommodations in this class must obtain an accommodation letter from Student Disability Services, 385 Garland, (410) 516-4720, studentdisabilityservices@jhu.edu .

ABET Outcomes

- An ability to apply knowledge of computing and mathematics appropriate to the discipline (a)
- An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution (b)
- An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs (c)
- An ability to function effectively on teams to accomplish a common goal (d)
- An understanding of professional, ethical, legal, security and social issues and responsibilities (e)
- An ability to communicate effectively with a range of audiences (f)
- An ability to analyze the local and global impact of computing on individuals, organizations and society (g)
- Recognition of the need for and an ability to engage in continuing professional development (h)
- An ability to use current techniques, skills, and tools necessary for computing practice (i)
- An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices (j)
- An ability to apply design and development principles in the construction of software systems of varying complexity (k)