Introduction to Computer Security (ECE 4115) - Spring 2017

Meeting times / place:

When: 9:35 am - 10:55 am TR

Where: Klaus 2443

Instructor Course Summary Textbooks References
Grading & Policies Labs Schedule

Instructor

Instructor: Dr. Raheem Beyah	
Office	Klaus 2308
Office hours	TR 11am - noon
Email	raheem.beyah@ece.gatech.edu

Teaching Assistant: Caleb Purcell	
Email	cpurcell3@gatech.edu
Lab Information	

Course Summary

The course covers introductory topics in computer security. The goal is to expose students to fundamental security primitives and to a broad range of current security challenges. The course provides a hands-on approach to examining a wide range of topics in operating systems, software engineering, and network and communications security.

Students will work with various tools and techniques used by hackers to compromise computer systems or otherwise interfere with normal operations. The purpose of the class is NOT to teach you how to be a hacker, but rather to teach you the approaches used by hackers so you can better defend against them. Students work in groups of two to complete assigned labs. It is OK to talk to others and help each other in the lab. Students will be graded based upon exams and completion of assigned labs.

Lab Rule:

You will NEVER take any programs from the lab on any writable media/memory devices, nor will you ever connect any of the lab machines to any production wired or wireless network machines or laptop devices. This is to prevent the spread of any of our malicious programs and techniques. You are encouraged to bring code into the lab to experiment with.

Policy on Commenting Software:
Fully commenting code, even code that you were given as a starting point is mandatory. This is one of the instructor's pet peeves. You must fully comment all code you turn in and must include comments to explain all of the code you turn in. (Even those parts of the code you did not write but were given as a starting point). You must include in the comments an explanation of what the purpose of the code is, the date the code was originally written, the date the code was last modified, your lab team member names and your group number must be in the comments. The last date modified must be correct and in the comments.

Policy on Handouts:
The handouts and lecture notes for 4894 can be downloaded from the class web page (this document) which is password protected. Handouts with proprietary or copyrighted material will be put on the protected page and should not be made publicly available by students.

Prerequisites: ECE3076 or ECE3600 or ECE 4110 or CS3251; some previous C Programming (or Java) experience would be beneficial

Learning Objectives

1. Understand fundamental network and computer security primitives.
2. Understand practical challenges and solutions related to network and computer security.
3. Apply their knowledge of computer architecture, operating systems, and computer networks to analyze system and network attacks.
4. Demonstrate the ability to use sophisticated laboratory hardware- and software-based networking and system analysis tools.

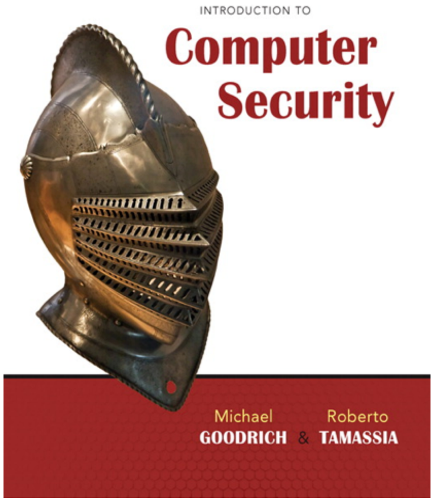
Learning Outcomes

1. Describe why system and networks are vulnerable to attacks.
2. Describe various methods for defending and detecting system and network attacks.
3. Understand practical challenges with implementing and defending against system and network attacks.
4. Understand how to utilize hardware- and software-based networking and system analysis tools.
5. Prepare laboratory reports and documentation conforming to appropriate technical standards.

Textbooks

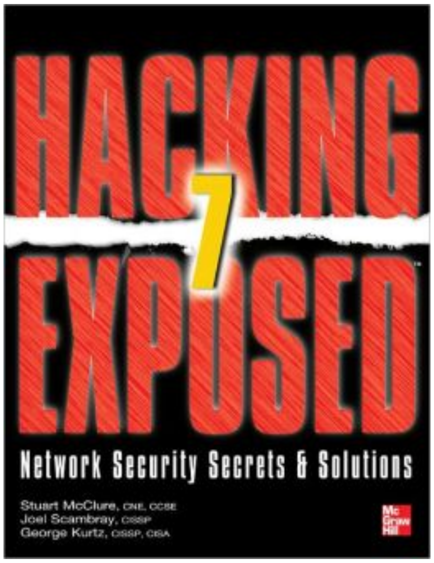
There is one required textbook and one recommended textbook. We cover lots of really good material and no one textbook has it all. These are excellent references and will serve you well in future jobs or research projects. We will also occasionally review conference and journal publications.

Text One: Required



Introduction to Computer Security, by Goodrich and Tamassia, ISBN: 978-0321512949

Text Two: Recommended


HACKING
7
EXPOSED
Network Security Secrets & Solutions
Stuart McClure, CNE, CCSE
Joel Scambray, CISSP
George Kurtz, CISSP, CISA
Mc Graw Hill

Hacking Exposed 7: Network Security Secrets & Solutions (SEVENTH EDITION), by McClure, Scambray, and Kurtz, ISBN 978-0071780285

References

Security:

- Counter Hack Reloaded, Second Edition, Ed Skoudis, Prentice Hall, ISBN 0-13-148104-5
- Gray Hat Hacking The Ethical Hackers, Third Edition, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, ISBN 0-071-74255-7
- Hands-On Ethical Hacking and Network Defense, Michael Simpson, Thompson, ISBN 0-619-21708-1
- The Unofficial Guide to Ethical Hacking, Second edition, Ankit Fadia, Thomson Course

Technology, ISBN 1-59863-062-8

- Rootkits, Subverting the Windows Kernel, Greg Hoglund and James Butler, Addison Wesely, ISBN 0-321-20098-5

TCP/IP and Internets in General:

- IP Fundamentals, by Thomas Maufer ISBN 0-13-975483-0
- Internet Core Protocols, Eric Hall and Vint Cerf, O'Reilly, ISBN 1-56592-572-6
- TCP/IP Illustrated The Implementation, Volume 2, Gary R. Wright and Richard W. Stevens, ISBN 978-0201633542

LINUX Internet Implementation:

- TCP/IP and Linux Protocol Implementation, John Crowcroft and Ian Phillips, Wiley, ISBN 0-471-40882-4
- Linux IP Stacks Commentary, Coriolis Open Press, By Maxwell, ISBN 1-576-10470-2
- Linux Core Kernel Commentary, Second Edition, Coriolis Open Press, By Maxwell, ISBN 1-588-80149-7

Internet Programming:

- The Pocket Guide to TCP/IP Sockets, C Version, Donahoo and Calvert, Morgan Kaufman, ISBN 1-55860-686-6
- Beginning LINUX Programming, by Neil Matthew and Richard Stones, WROX Press,ISBN 1-874416-68-0
- UNIX Network Programming Interprocess Communications, Volume 2, SECOND EDITION, Richard Stevens, ISBN 978-0130810816
- Internetworking with TCP/IP Client-Server Programming and Applications, Volume III, Douglas E. Comer and David L. Stevens, ISBN 978-0130320711

Intrusion Detection:

- Intrusion Signatures and Analysis, Northcutt, Cooper, Fearnow and Frederick, New Riders, ISBN 0-7357-1063-5
- Network Intrusion Detection An Analyst's Handbook, Second Edition, New Riders, ISBN 0-7357-1008-2

Grading & Policies

Grading	
Labs	30%
Midterm 1	20%
Midterm 2	20%
Final Exam	30%

Grading Scale	
90% - 100%	A
80% - 89%	B
70% - 79%	C
60% - 69%	D

Total	100%

< 60%	F

Responsibility for Material:

Students are responsible for all material in assigned sections of texts, even if not explicitly covered in lecture. Students are also responsible for all material covered in lecture.

Exams, Makeup Exams, and Incompletes:

All exams are closed book. As a rule, makeup exams will be offered at the discretion of the professor and only for scheduled absences that are requested in writing at least one week in advance. Medical emergencies are the only exception to this rule and in case of such an emergency, the student must contact the professor as soon as possible to discuss the makeup. Incomplete grades will be given only in extraordinary circumstances.

Late Turn-in and Re-grading:

Labs can be turned in two days after the due date and will be subject to a 20% penalty. The grade for the lab will be zero after this window. Exams will not be considered for re-grading later than the next class period after they are returned. Re-grading requests should be submitted in writing with a specific explanation of the possible grading error. Photocopies of completed exams will be made by the instructor prior to returning them.

Academic Honesty:

Although students are encouraged strongly to communicate with each other to assist in learning the course material, all students are expected to complete course work individually (unless instructed otherwise), following all instructions stated in conjunction with exams and assignments. All conduct in this course will be governed by the Georgia Tech honor code. Additionally, it is expected that students will respect their peers and the instructor such that no one takes unfair advantage of any other person associated with the course. Any suspected cases of academic dishonesty will be reported to the Dean of Students for further action.

Excused Absence Policy

Link

Disability Services Statement

If needed, we will make classroom accommodations for students with documented disabilities. These accommodations must be arranged in advance and in accordance with the Office of Disability Services Link

Labs

The laboratory is in the Klaus building, room 2446. It will be manned by the teaching assistant based on the schedule below.

Contact Information	
Teaching Assistant	**Caleb Purcell**

Email	cpurcell3@gatech.edu
Labs	Klaus 2446
Lab Hours	Tuesday 1:30 pm - 4:30 pm
	Wednesday 1:30 pm - 4:30 pm
	Thursday 1:30 pm - 4:30 pm
	Friday 1:30 pm - 4:30 pm

The laboratory assignments will be on the following subjects:

- Reconnaissance, Network Mapping, Vulnerability Assessment
- Password Cracking, Network Sniffing, Man-in-the-Middle Attacks, and Virtual Private Networks
- Address Spoofing, Denial of Service, Email Spoofing, and VoIP
- Firewalls
- Rootkits, Backdoors, and Trojans
- Buffer Overflow attacks
- Honeynets
- Worms and Viruses
- Web Security
- Botnets

Link to class Piazza site:

Schedule

A tentative schedule of lectures (subject to change) is provided below.

Week 1, Jan 5th

Topic(s): *Course Overview and Introduction* , *Ethical Hacking*

- Ethical Hacking
- Introduction and Overview
- Fundamental Concepts

Reading(s):

- Class: Goodrich (Chapter 1)
- Lab:
  - S. A. Shaikh, H. Chivers, P. Nobles, J. A. Clark, Hao Chen. Network reconnaissance. Network Security, Volume 2008, Issue 11, 2008. [PDF]
- Supplemental Material:
  - B. Cheswick. An Evening with Berferd in which a cracker is lured, endured, and studied. Usenix, 1992. [PDF]

[Lab 1: Reconnaissance, Network Mapping, Vulnerability Assessment]

- - Assigned: January 8th, Due: January 17th

Week 2, Jan 12th

Topic(s): Network Security

- Network Security Concepts
- Attacks at Multiple Layers and Countermeasures
- Denial-of-Service Attacks
- Firewalls
- Intrusion Detection
- Wireless Networking Concepts, Attacks, and Countermeasures

Reading(s):

- Class: Goodrich (Chapter 5)
- Lab:
- Supplemental Material:

[Lab 2: Password Cracking, Network Sniffing, Man-in-the-Middle Attacks, and Virtual Private Networks] - - Assigned: January 17th, Due: January 29th

Week 3, Jan 19th

Topic(s): Network Security

- Network Security Concepts
- Attacks at Multiple Layers and Countermeasures
- Denial-of-Service Attacks
- Firewalls
- Intrusion Detection
- Wireless Networking Concepts, Attacks, and Countermeasures

Reading(s):

- Class: Goodrich (Chapters 5, 6)
- Lab:
- Supplemental Material:

Week 4, Jan 26th

Topic(s): Network Security

- Network Security Concepts
- Attacks at Multiple Layers and Countermeasures
- Denial-of-Service Attacks
- Firewalls

- Intrusion Detection
- Wireless Networking Concepts, Attacks, and Countermeasures

Reading(s):

- Class: Goodrich (Chapters 6)
- Lab:
- Supplemental Material:

[Lab 3: Address Spoofing, Denial of Service, Email Spoofing, and VoIP] - - Assigned: January 29th, Due: February 7th

Week 5, Feb 2nd

Topic(s): Operating Systems Security

- Operating Systems Concepts Overview
- Process Security
- Memory and Filesystem Security
- Application Program Security

Reading(s):

- Class: Goodrich (Chapter 3)
- Lab:
- Supplemental Material:

[Lab 4: Firewalls] - - Assigned: February 7th, Due: February 19th

Week 6, Feb 9th

Topic(s): Operating Systems Security

- Operating Systems Concepts Overview
- Process Security
- Memory and Filesystem Security
- Application Program Security

Reading(s):

- Class: Goodrich (Chapter 3)
- Lab:
- Supplemental Material:

[Lab 5: Rootkits, Backdoors, and Trojans] - - Assigned: February 19th, Due: February 28th

Tuesday, February 10th

Exam 1 - Sample Exam

Week 7, Feb 16th

Topic(s): *Malware*

- Insider Attacks
- Computer Viruses
- Malware Attacks
- Privacy-Invasive Software
- Countermeasures

Reading(s):

- Class: Goodrich (Chapter 4)
- Lab:
- Supplemental Material:

Week 8, Feb 23rd

Topic(s): *Malware*

- Insider Attacks
- Computer Viruses
- Malware Attacks
- Privacy-Invasive Software
- Countermeasures

Reading(s):

- Class: Goodrich (Chapter 4)
- Lab:
- Supplemental Material:

[Lab 6: Buffer Overflow attacks] - - Assigned: February 28th, Due: March 12th

Week 9, March 2nd

Topic(s): *Web Security*

- The World Wide Web Overview
- Attacks on Clients
- Attacks on Servers

Reading(s):

- Class: Goodrich (Chapter 7)

- Lab:
- Supplemental Material:

Week 10, Mar 9th

Topic(s): Cryptography

- Symmetric Cryptography
- Public-Key Cryptography
- Cryptographic Hash Functions
- Digital Signatures

Reading(s):

- Class: Goodrich (Chapter 8)
- Lab:
- Supplemental Material:

[Lab 7: Honeynets] - - Assigned: March 12th, Due: March 26th

SPRING BREAK, Mar 16th

Week 11, Mar 23rd

Topic(s): Cryptography

- Symmetric Cryptography
- Public-Key Cryptography
- Cryptographic Hash Functions
- Digital Signatures

Reading(s):

- Class: Goodrich (Chapter 8)
- Lab:
- Supplemental Material:

[Lab 8: Worms and Viruses] - - Assigned: March 26th, Due: April 4th

Monday, March 30th

Exam 2 - Sample Exam

Week 12, Mar 31st

Topic(s): Security Models and Practice / Miscellaneous Topics

- Kerberos

- Social Networking Security

Reading(s):

- Class:Goodrich (Chapter 7)
- Lab:
- Supplemental Material:

[Lab 9: Web Security] - - Assigned: April 4th, Due: April 11th

Week 13, April 6th

Topic(s): Usable Security

- TBD
- TBD

Reading(s):

- Class: TBD
- Lab:
- Supplemental Material:

[Lab 10: Botnets] - - Assigned: April 11th, Due: April 18th

Week 14, April 13th

Topic(s): Privacy

- TBD
- TBD

Reading(s):

- Class: TBD
- Lab:
- Supplemental Material:

Week 15, April 20th

Topic(s): Course wrap up - Makeup

- TBD
- TBD

Reading(s):

- Class: TBD
- Lab:

- Supplemental Material:

Tuesday, April 28th

FINAL EXAM (8:00am - 10:50am)