COSC 734-101: Network Security

Instructor: Dr. Wei Yu

Email: wyu@towson.edu

Office: YR 467

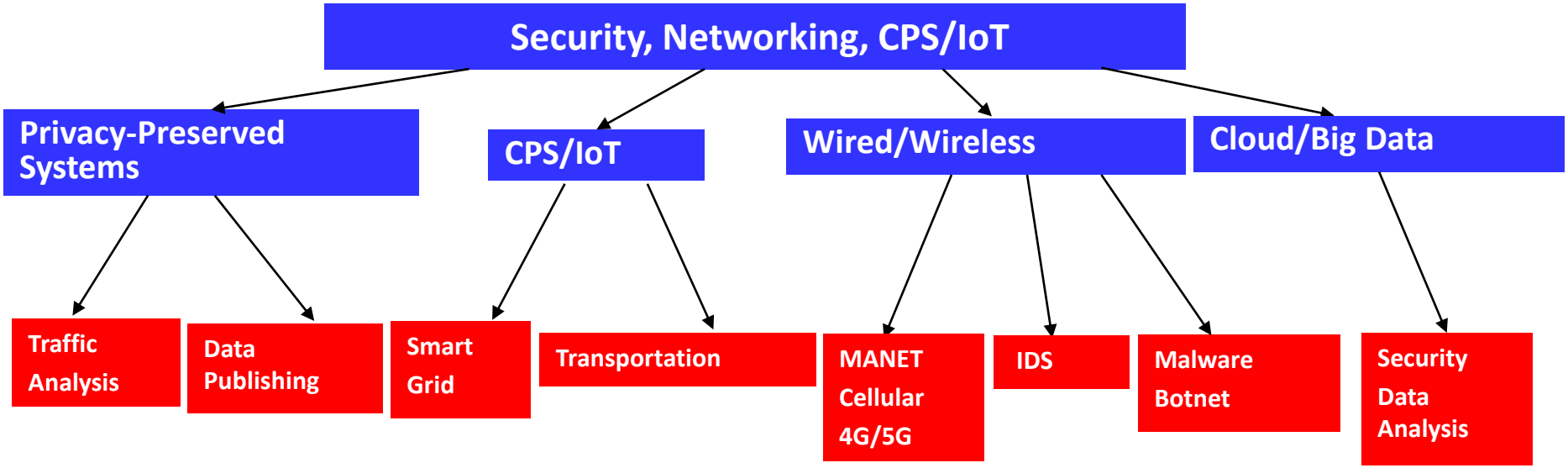
Howdy!

- This course will provide an introduction to concepts of network security principles and applications to understand the techniques that detect, prevent, and mitigate such occurrences.
- Topics include
  - System security (intrusion detection, malicious software, firewall and others)
  - Basis of cryptography and examples to secure protocols
  - Network security applications (key management, transport level security, wireless network security and IP security)
- Background: introduce yourself and your (research) interest/ background
  - Let me and other students know more about you
  - To find potential research term project

Dr. Wei Yu Experiences

- Education
  - Ph.D. (Computer Engineering) from Texas A&M University
  - BS (CE), MS(EE)
- Working experience
  - Worked for Cisco Systems Inc almost nine years
  - Developed software in the areas of VoIP and telecommunication
- Research Interests
  - Cyber Space Security, Computer Networks and Cyber-Physical Systems/Internet-of-Things, Distributed Computing
- Publications
  - Over 200 papers in various journals and conferences
    - IEEE Symposium on Security and Privacy (S&P), ACM Computer and Communication Security (CCS), INFOCOM, ICDCS
    - IEEE Transactions on Networking (ToN), IEEE Transactions on Parallel & Distributed Systems (TPDS), IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Computers (TC), IEEE Transactions on Mobile Computing (TMC), and IEEE Transactions on Transactions on Vehicular Technology (TVT)

Research Roadmap



Our Research Group

Research Lab Environment

Research Highlights

- **Well Funded Research in Cyber Security, Network, CPS/IoT by federal agencies**
  - Research awards as PI over 2 million
  - Information assurance scholarships and capacity building awards as co-PI over $2.3 million
- **Key Achievements**
  - Recipient of the USM Wilson H. Elkins Professorship
  - Recipient of the USM Regent's Award for Scholarship, Research, or Creative Activity, 2015
  - Recipient of NSF CAREER Award, 2014
  - Three best paper awards (2016 IEEE IPCCC, 2013 IEEE ICC, and 2008 IEEE ICC)
  - Establishing collaboration with NIST, ARL, AFRL, etc.
  - 2012 Excellence in Scholarship Award from Fisher College of Science and Mathematics at Towson
  - Near 200 research journal and conference publications
  - Advised 16 doctoral students (5 graduated/11 ongoing – 4 joined universities as tenure-track assistant professor) and 24 master students in research projects

More Information

https://wp.towson.edu/wyu/

Funding Sources and Collaborations

- **CPS/IoT**
  - National Science Foundation (CAREER Award)
  - National Institute of Standards Technology (NIST)
  - University System of Maryland (USM)
- **Mobile and Wireless Networks and Security**
  - Army Research Laboratory
  - National Institute of Standards Technology (NIST)
- **Network Threat Monitoring and Detection**
  - Air Force Research Laboratory
- **Privacy and Anonymized Systems**
  - National Science Foundation

Next Projects?

- Public Safety Communication Network
- Edge Computing
- Big Data and Trading
- ???

Basic SIP Call Setup & Teardown

10.19.150.2

10.19.150.6

User Dials IP Phone @ 10.19.150.6

SIP Message INVITE

100 Trying SIP Response

180 Ringing SIP Response

200 OK SIP Response

User Answers

SIP Message ACK

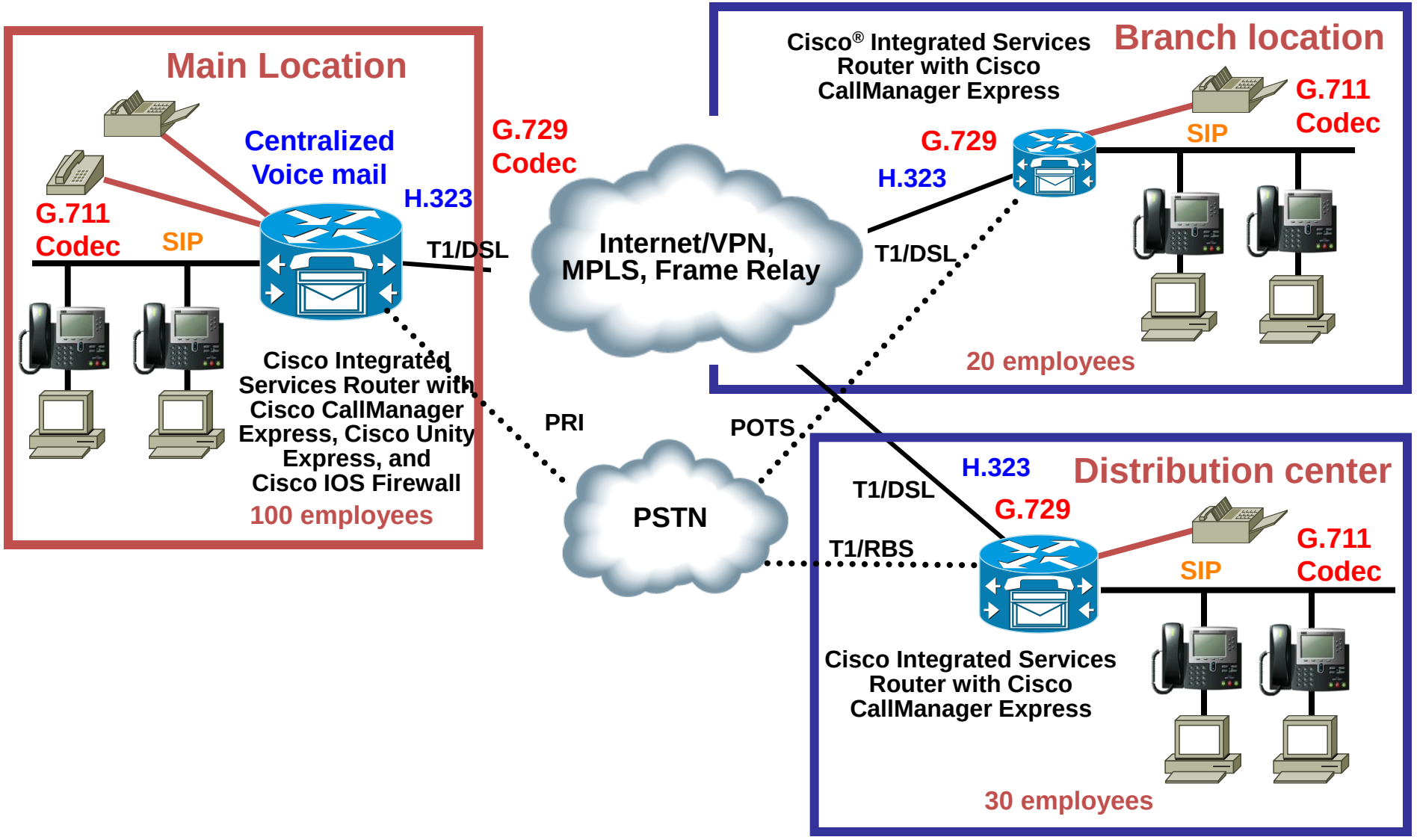
RTP Media Flow

User Hangs Up

SIP Message BYE

200 OK SIP Response

Multi-site VoIP Networking



Course Overview

What This Course About

- Introductory course
  - Introduce concepts and principles underlying network security
  - Provide the understanding of relevant techniques
  - Understand the various ways that information and network systems and applications can be compromised
  - Learn ways to understand the risk and prevent detect and mitigate threats and attacks
- A few advanced subjects to discuss
  - New development in network security
- Great for those
  - Interested to know more about network security
  - Interested to conduct network security research

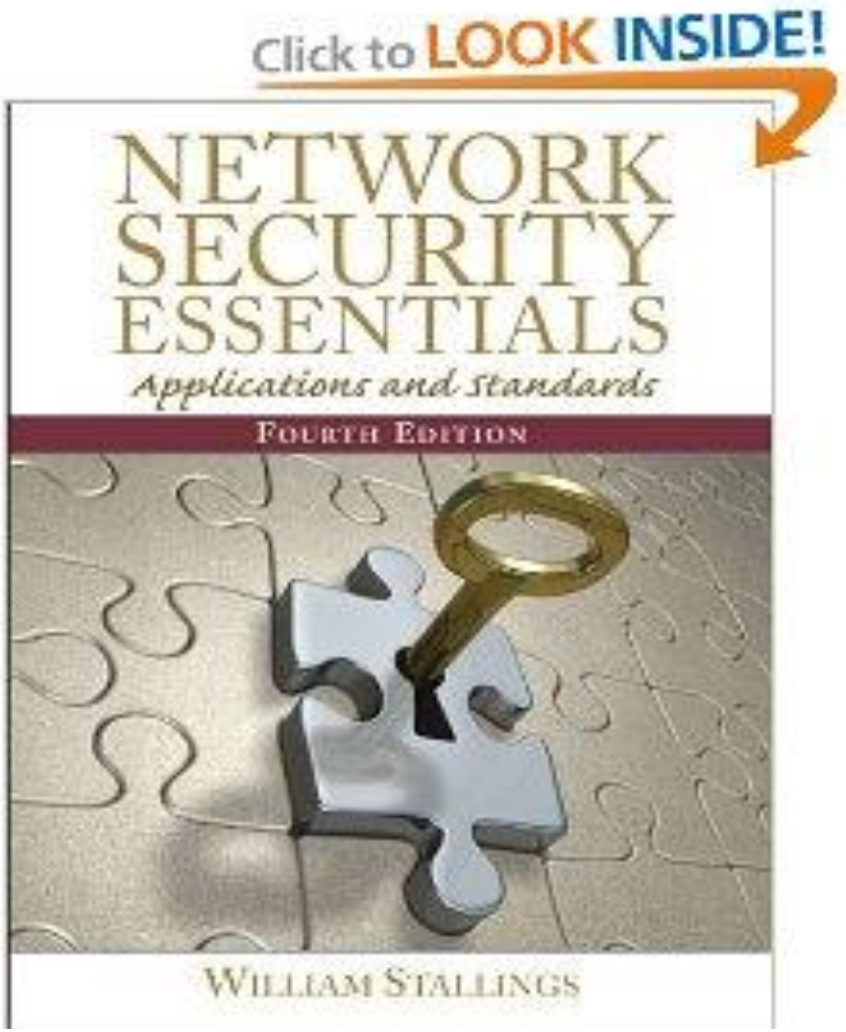
Prerequisites

- The **motivation to learn and explore the problems**
- Knowledge of networking, algorithm design, operating systems, and programming (C or C++ or Java)
  - COSC 600 (Adv File & Data Systems), COSC 650 (Network)

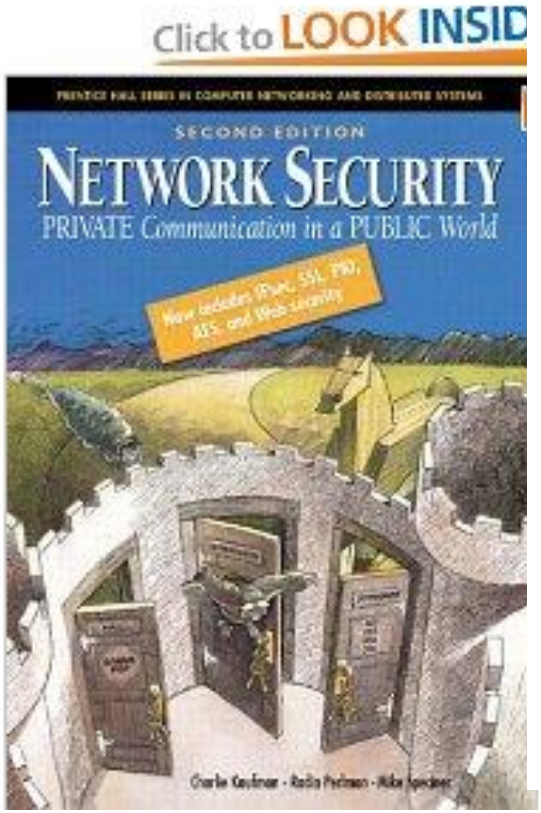
Teaching Material

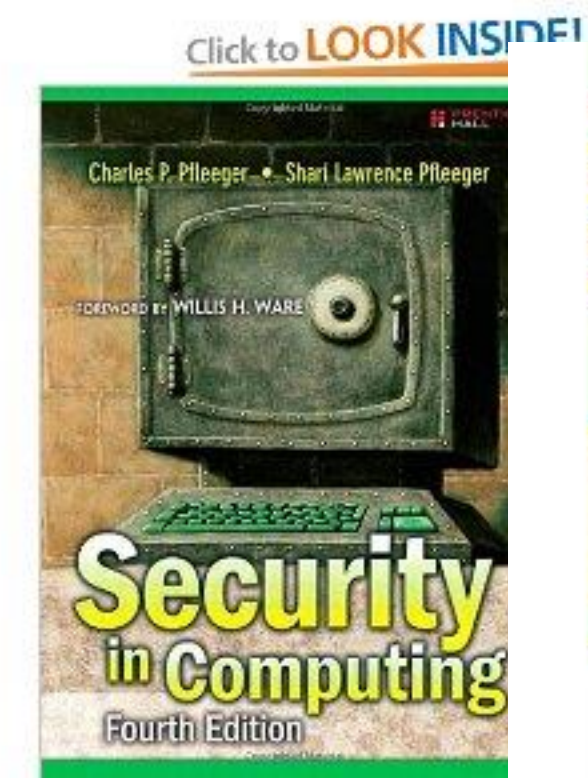
- Required Textbook
  - **William Stallings, Network Security Essentials, Fourth Edition, Prentice Hall, 2011. ISBN-10: 0-13-610805-9 (required)**
- Other References:
  - Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security - Private Communication in a Public World, 2/E, 2002, Prentice-Hall. ISBN 0-13-046019-2.
  - Charles P. Pfleeger and Shari Lawrence Pfleeger. Security in Computing, Fourth Edition. Prentice Hall, 2007. ISBN 0-13-239077-9.
  - Matt Bishop, Introduction to Computer Security, Addison-Wesley, 2004. ISBN 0-321-24744-2.
- Some research papers published in top security conferences and journals

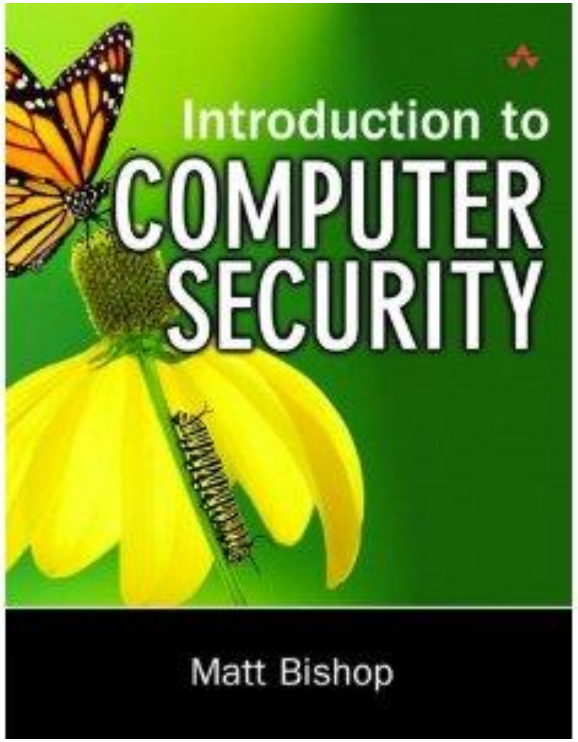
Textbook


Click to LOOK INSIDE!
NETWORK SECURITY ESSENTIALS
Applications and Standards
Fourth Edition
William Stallings

References


Click to LOOK INSID
SECOND EDITION
NETWORK SECURITY
PRIVATE Communication in a PUBLIC World


Click to LOOK INSIDE!
Charles P. Pfleeger • Shari Lawrence Pfleeger
FOREWORD BY WILLIS H. WARE
Security
in Computing
Fourth Edition


Introduction to
COMPUTER
SECURITY
Matt Bishop

Conferences

- ACM SIGCOMM (ACM SIG on Communications)
- IEEE INFOCOM (IEEE International Conference on Computer Communications)
- IEEE ICDCS (International Conference on Distributed Computing Systems)
- IEEE S&P (IEEE Symposiums on Security and Privacy)
- ACM CCS (ACM Conference on Computer and Communications Security)
- IEEE ICNP (IEEE International Conference on Network Protocol)
- Others

Journal

- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- ACM Transactions on Information and System Security
- IEEE Transactions on Networking
- IEEE Transactions on Distributed and Parallel Systems (TPDS)
- IEEE Transactions on Mobile Computing (TMC)
- IEEE Transactions on Computers (TC)
- Others

Course Requirements

- Assignments
  - Around 3-4 assignments: reviewing review, solving problems on textbook, and/or lab assignments
  - All problem sets are due at the time and date specified on the assignment
- Survey paper
  - Select a related subject, read over 20-30 related research papers, and develop a survey paper with 6-8 pages.
- Research project and project report
  - Study an assigned topic related to network security
  - Write a short (conference style) paper (6-8 pages based on IEEE conference format; template will be posted on line)
  - Make a presentation (20 minutes) to show the results of your research project
  - Paper and presentation details will be given later
- Exams
  - Final Exam (May 18 - Thursday, 7:30pm-9:30pm))

Grading

- Students will be evaluated on the following basis:
  - Assignments: 20%
  - Research project: 25%
  - Paper survey: 15%
  - Presentation: 10%
  - Participation: 10%
  - Final exam: 20%
- Course grades will be assigned as follows:

  A=90-100%, B=80-89%, C=70-79%, F=0-69%

One Type of Assignments: Paper Reviewing

- You need to write a review for the assigned paper
- Review can include:
  - Problem domain: background, motivation, why this problem important/novel/interesting
  - Idea of the paper: assumption, main techniques, results
  - Comparison with related work
  - Possible future work/direction
  - Pros, cons of the paper (your conclusion)
  - What can we do based on this work: lesson learned from this work?
  - Stimulate new related problem? Flawed assumption/technique can be improved/extended? technique can be used to other (maybe your own dedicated) domain to solve other problem? what extension can we do for further work?

More Assignments

- You will be given some problems related to algorithms and protocols based on the textbook we discuss during the class.
  - Examples: intrusion detection, firewall rule setting, authentication protocols, etc.
- You will give work on the lab assignments
  - Because the lab environment is virtual machine based, you can do it at YR 405 or using your own PC
  - The VM image will be provided
  - Examples:
    - Implement Packet Sniffing Program and conduct network spoofing;
    - Study attacks against TCP protocols;
    - Study performance of crypto algorithms;

Survey Paper

- Need to be done independently
- Find a research topic and read at 20-30 research papers
- Write a literature review
- Will give an example to show you how to write survey paper

Survey Paper Report Due on May 19th

Research Project

- Need work on it independently, but you can discuss your topic with other students
- Select one topic from the list or you can select your own subject my approval (I will post the list of topics in the blackboard)
  - **Send me an email about your selection by 02/24**
- After selecting a project subject, I may give some papers to students for select topics
- Each student needs to report his/her project progress regularly (1-on-1 or email)
- Each student needs to present and deliver the final research project (6-8 pages based on IEEE transactions standard template)
- Students need to learn and use latex to rewrite you survey and project report
- There will be BONUS points for excellent projects

Final Research Project Report Due May 19th

Presentation

- You need to read deeply in the given papers
- As a paper presenter, you should
  - Prepare slides
  - Present to the class
  - Steer the extensive discussion
  - Prepare a list of discussion questions on the topic/papers

Schedule

Week	Date	Topic	Chapter
1	2/2	Course Introduction	
2	2/9	Overview	Ch. 1
3	2/16	Intrusion Detection	Ch. 9
4	2/23	Malicious Software	Ch. 10
5	3/2	Internet Global Threats and Defense	
6	3/9	Firewall	Ch. 11
7	3/16	Symmetric Encryption/ Public-key Cryptograph	Ch. 2/3
8	3/23 (No class)	Spring Break (No class)	
9	3/30	Key Distribution & Authentication	Ch. 4
10	4/6	Advanced Topic	
11	4/13	Advanced Topic	
12	4/20	Advanced Topic	
13	4/27	Student project presentation	
14	5/4	Student project presentation	
15	5/11	Student project presentation	
		Student project report due on 5/19 Final Exam (May 18, 7:30pm-9:30pm)	

Conference/ Journal in Security Area

- Top Conferences
  - IEEE S&P (IEEE Symposiums on Security and Privacy)
  - ACM CCS (ACM Conference on Computer and Communications Security)
  - Usenix Security Symposium (Security)
  - Annual Network and Distributed System Security Conference (NDSS)
  - IEEE INFOCOM, ICDCS
  - …
- Journals
  - IEEE Transactions on Information Forensics and Security (TIFS)
  - IEEE Transactions on Dependable and Secure Computing (TDSC)
  - ACM Transactions on Information and System Security (TISSEC)
  - IEEE Transactions on Networking (ToN)
  - IEEE Transactions on Computers (TC)
  - IEEE Transactions on Parallel and Distributed Systems (TPDS)
  - …