Network Security

AA 2020/2021

Welcome to the course

Prof. Bruno Crispo

This course [145065]

- This is a 6 credits course
  - They are 6 well deserved credits

- This is a MSc course
  - Students are supposed to *proactively* interact with the class and the learning activity
  - Students are supposed to apply what they learn to new problems, deal with complexity and use scientific papers.
  - Students are expected to *work throughout the course*
    - *As opposed to solely the final rush 5 days before the exam*
  - Theory + Laboratory

What this course is and is not

- This course is
  - This course aims at giving you **both** a theoretical and practical view of Network Security aspects
  - This course's learning leans toward
    - Cutting-edge aspects of NetSec
    - Production of original knowledge from the students
- This course is not
  - A course on crypto / channel security / cyphers
  - A theoretical course where you will be taught and asked for the formal implementation details of, e.g. a cryptographic protocol
- For these reasons there is **no prescribed text book**
  - Learning happens in class, reading the provided material, during discussion with students, in the lab.

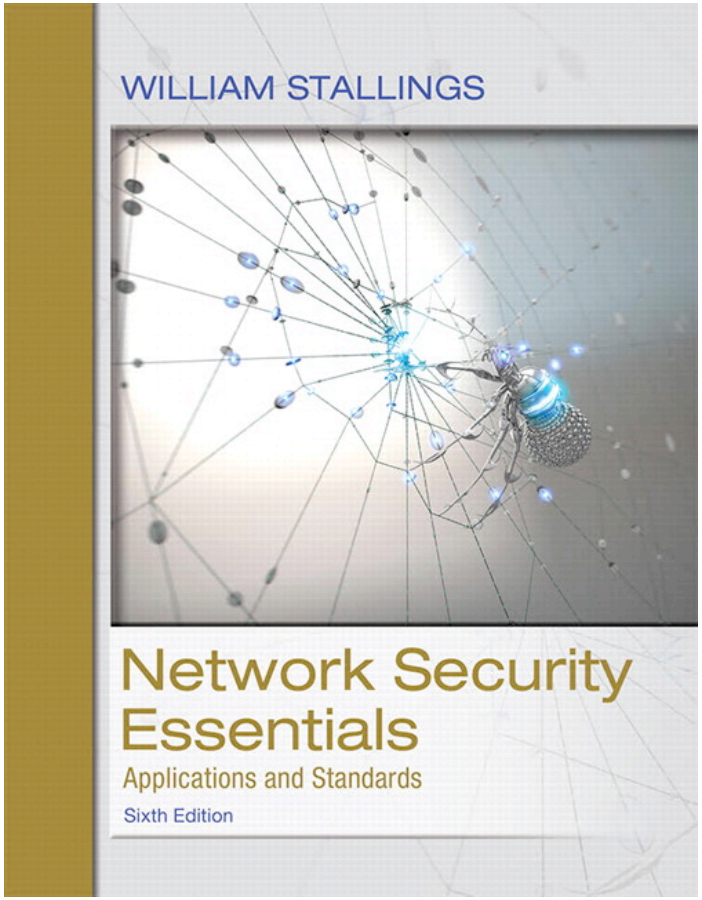
Support textbook

Network Security Essentials: Applications and Standards, 6th Edition
William Stallings

Publisher: Paerson

+ Security Engineering, 2nd edition
Ross Anderson
Available online
http://www.cl.cam.ac.uk/~rja14/book.html

+ all scientific papers indicated during the lectures



Learning objectives

- Learning objectives are twofold
  - You learn the technical fundamentals of network security, that include the most common network attacks and attack approaches as well as the most common detection, prevention and mitigation network security techniques. You will do that by mean of theoretical lectures and practical assignments.
  - You learn soft skills on how to design a lab lecture and how to present it to your peers. How to write a report.

The lecturer

- Bruno Crispo (bruno.crispo@unitn.it)
  - MSc in Networking from University of Turin
  - PhD in Computer Security from Cambridge University, UK
  - Currently Full Professor at the University of Trento and visiting professor at KU Leuven, Belgium.
    - Previous appointments:
    - Vrije Universiteit Amsterdam
    - Stanford Research Institute, Telecom Italia Labs
    - My own company: Cryptomathic Italia SpA
  - Current research activities:
    - Web Security
    - IoT security and privacy
    - Mobile platforms security and behavioral biometrics
    - Bit and pieces on access control, network security, OSN security, etc.
  - Graduated 16 PhD, supervising now 5, supervising several MSc final projects. Numerous connections with industry.
  - Several publications, presentations, seminars, etc.
  - Always looking for good PhD candidates

The Teaching Assistant (TA)

- Dr. Michele Grisafi (michele.grisafi@unitn.it)
  - PhD of mine working in the area of IoT security and system security.
  - Solid skills in programming and sys admin

Learning Verification

- Grading structure of the verification:
  - Final grade:
    - 20 points written exam
    - 1 point for the first assignment
    - 12 points lab assignment

- **Any of the following will cancel all of your points and result in a rejection at the exam + possible action on side of University**
  - Plagiarism (for **any** assignment)
  - Cheating on the exam

Course organization

- The course is split in two "chunks" or parts
  1. Theoretical part → teaching (**lecturer holds the class online**)
  2. Laboratory part → student classes (as in "**the student holds the class online**"). Lab part is mandatory and you **must** attend
- During part (1) we will explore problems, solutions, and limitations of network and computer security → **Written exam**
- The students will form working groups
- For part (2), each group picks up a topic among those seen in class
  - Builds a laboratory for each group to attend online → **Lab exam**
    - e.g. Build IDS signatures/IDS evasion, social engineering, Web attacks, etc…
  - Grade depends on quality of
    - LAB presentation, report
    - LAB activity

The laboratory part

- Due to restrictions as consequence of the Covid-19 we transformed the malware lab in a virtual lab
- So instead of using the Malware Lab, the lab will be prepared and performed on the student's computer
- Each group will do the presentation online using Zoom in synchronous mode and all students must participate to the online meeting

Course program (part 1)

- Introduction
  - Network security fundamentals
  - Attacker Models
- Network aspects
  - TCP/IP protocol 101
  - IPSec
  - Contact tracing
- Vulnerabilities
  - Configuration vulnerabilities and attack surfaces
  - Vulnerabilities in software
  - Vulnerability management
- Attacks
  - Network attacks
  - Malware
  - Drive-by downloads & exploit kits
  - Botnets
- Defensive technologies
  - System hardening
  - Firewalls
  - IDSs
  - Advanced memory techniques
- Privacy in networks
  - Honest-but-curious attackers
  - Tracking/fingerprinting
  - Applications of crypto
  - VPNs/TOR

Course schedule

- Course period
  - 2 March 2021 – 9 June 2021 (skip 17/3 and 2/6)
- Two classes per week
  - Tuesdays 9.30-11.30 online zoom
  - Wednesday 9.30-11.30 online zoom
- Then they will became two labs per week (unless we need to duplicate lab classes)

- Link Zoom Meeting
- https://unitn.zoom.us/j/4029679640
- Meeting ID: 402 967 9640 Passcode: 148730

Tentative course schedule (topics are indicative)

NetSec Tuesday 9.30-11.30
Wednesday 9.30 - 11.30

date		topic		
2.03.2021			intro/sec properties	
3.03.2021			net sec aspect	
9.03.2021			net sec aspect	
10.03.2021			netsec protocols	admission to the course and malware lab
16.03.2021			contact tracing	
17.03.2021	Degrees			list of topics for the lab
23.03.2021			vulnerabilities	
24.03.2021			vulnerabilities	groups formation and topic selection
30.03.2021			malware	
31.03.2021			malware	4 weeks lab preparation and meetings with lecturer
6.04.2021			firewalls	
7.04.2021			ids	
13.04.2021			ids	
14.04.2021			lab meetings	
20.04.2021			webattacks	
21.04.2021			privacy/TOR	
27.04.2021			Ghidra/Khali	
28.04.2021		lab1		
4.05.2021		lab2		attendance to the lab is mandatory
5.05.2021		lab3		
11.05.2021		lab4		
12.05.2021		lab5		
18.05.2021		lab6		
19.05.2021		lab7		
25.05.2021		lab8		
26.05.2021		lab9		
1.06.2021		lab10		
2.06.2021	Holiday			
8.06.2021		lab11		
9.06.2021		lab12		

More on the laboratory part

- Students that want to do the lab must register to the course by 9th of March (Google Classroom)
- Students that want to do the lab project **must pass** the first assignment
- Students that want to do the lab project must form groups and choose the topic by the 23rd of March
- All students will have at a minimum 4 weeks to prepare their lab activity
  - Book your presentation slot
- Lab activities **can not overlap**
  - Topics assigned on a **first comes first served** basis
  - e.g. 2 groups want to do IDSs?
    - 1 uses Snort
    - 1 uses Zeek
- Example of topics (you can suggest your own → subject to approval):
  - Defense → IDS, Firewalls, Sys hardening
  - Attacks → BoF; SQLi; XSS; Malware eng; MitM; DDoS
- Labs are part of the course → all students must attend

Appointments with the lecturer

- Fixed 1 hour slot every Wednesday after class upon request
  - Questions on the course
  - Feedback on the assignments
- Book your time by email
  - bruno.crispo@unitn.it
- If I am not available we will arrange a different time
- After choosing the lab topic, I will have a round of meetings with each group to tune and discuss the design of the lab activity

The class' website

- A credit goes to Dr. Luca Allodi for early version of the slides

- Announcements and assignments on Google Classroom
- **classroom.google.com**
  - Access with your UNITN credentials
  - Access class with code

mdp65hf

- You will be considered enrolled in the course only upon joining
- If you want to drop off, please unsubscribe
- On this website you will find
  - Updates on the classes + material
  - Assignments + deadlines
  - Info on the course
- A copy of the slides will be also available on Moodle as well as the video of the lectures

FIRST ASSIGNMENT

- You can find the assignment published on the classroom.

- Install a web server (any)
- Protect the access to a webpage by means of a password and a captcha (i.e., reCAPTCHA).
- Connect via browser to that captcha and password-protected webpage
- Sniff the traffic with wireshark, between browser and web server and capture the password
- Configure the web server to use mutual authentication using TLS and digital certificates you need to generate. Show that now the password cannot be eavesdropped
- Record a video of max 3 minutes showing your working solutions (the result of the sniffing with and without TLS), the configurations files, the digital certificates,
- Submit your video to the classroom
- Deadline 10th March at 15.00