Network Security

AA 2015/2016

Welcome to the course

Dr. Luca Allodi

This course [145065]

- This is a 6 credit course
  - The lectures are recorded to be used for the online version of the very same course
- This is a MSc course
  - Students are supposed to *proactively* interact with the class and the learning activity
  - 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

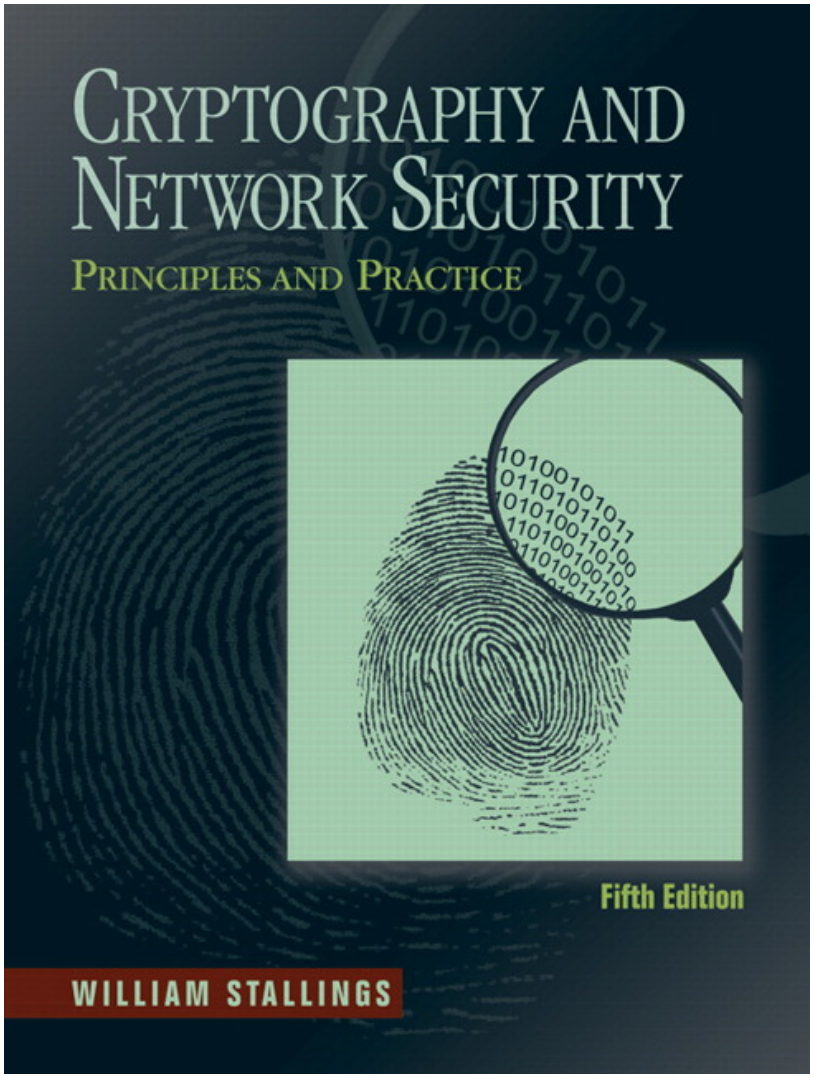
- This course is
  - This course aims at giving you **both** a theoretical and practical view of Network Security aspects
  - This course's learning leans toward
    - Cutting-edge aspects of InfoSec
    - Production of original knowledge from the students
- This course is not
  - A course on crypto / 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

"Cryptography and Network Security" 5/e
William Stallings

ISBN-10: 0136097049
Publisher: Prentice Hall International Edition

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



The lecturer

- Luca Allodi
  - MSc in Information Security from University of Milan
  - PhD in Information Security management from University of Trento
  - Currently research fellow at the University of Trento
    - Security management and policies
  - Member of the NIST/First.org consortium for the Common Vulnerability Scoring System
    - Worldwide standard for security vulnerability assessment
    - Worked with INTEL, Oracle, Juniper on its definition
      - (UNITN only European university involved, two world-wide)
  - Several publications, presentations, seminars, etc.

This course and the lecturer – Notes for the good student

- Grading structure:
  - Final grade:
    - 20 points written exam (35 with no lab assignment)
    - 15 points lab assignment (optional)
  - Periodic assignments for the students
    - 1-paragraph critical review of a research paper on aspects seen in class
    - Hand in your assignments in time
      - Late assignments will not be accepted
      - **If all assignments are in time and all assignments are good, +2 for final score**
- **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**)
2. Laboratory part → student classes (as in "**the student holds the class**")
- During part (1) we will explore problems, solutions, and limitations of Network and computer security → **Written exam**
- The students will form working groups of 2-3 people
- For part (2), each group picks up a topic among those seen in class
  - Builds a laboratory for each group to attend in class → **Lab exam**
    - e.g. Build IDS signatures/IDS evasion, write BoF exploit, Web attacks, etc…
  - Grade depends on quality of
    - LAB report
    - LAB activity

The laboratory part

- The second part of the course will be held entirely in the laboratory
- The “MalwareLab” (Povo 2, floor -2)
  - An isolated environment where you can play with attacks, defenses, virtual infrastructure
  - You will be granted access there upon signing an agreement of good conduct
    - Essentially: you are **fully responsible of any misuse of the tech in the lab**
- We will have a first lab activity together
  - Show you the lab and how to use it
  - Tutorial on Exploit Kits

Exam

- Two modalities
- First: Project + half written exam
  1. Project grading (15pnts) → assigned for organising a lab activity
     - Grade always valid unless `studentsRefuses(project.grade)`
     - One shot at this. You can't do a second project
  2. Written exam grading (20pnts) → June session
- Second: Full written exam (35 points)
  - Includes questions from the laboratory activities

```
IF (studentRefuses(project.grade)||NoProject){
   FullWrittenExam=TRUE;
};
ELSE{
   HalfWrittenExam=TRUE;
}
```

Course program (part 1)

- Introduction
  - Network security foundamentals
  - Attacker Models
- Network aspects
  - TCP/IP protocol 101
  - Channel crypto
  - HTTPS/SSL/TLS
- Vulnerabilities
  - Configuration vulnerabilities and attack surfaces
  - Web Vulnerabilities
  - Vulnerabilities in software
- 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
  - 15 Feb 2016 – 27 May 2016
  - Optionally extend till 1st June
- Two classes per week (A207)
  - Monday 11-13
  - Wednesday 09-11

Course schedule

date	class	topic		
15/02/2016	A207	Intro to course	**Legend**	
17/02/2016	A207	Security of Network procols - IP	Lectures	
22/02/2016	A207	Security of Network procols - TCP/App	Lab Activity	Labs classes up to 3 hrs
24/02/2016	A207	Crypto	Holiday	
29/02/2016	A207	Vulnerabilities & attack surfaces		
02/03/2016	A207	Vulnerability scoring		
07/03/2016	A207	Vuln Scoring class exercise		
09/03/2016	A207	Attacks - malware		
14/03/2016	A207	Attacks - web attacks		
16/03/2016	A207	Attacks - economy and infrastructure		
21/03/2016	A207	Defensive tech - Sys hardening		
23/03/2016	A207	Defensive tech - Network defense (FW)	Groups are formed and lab topics chosen	
28/03/2016		Easter		
30/03/2016	A207	Defensive tech - Network defense (IDS)		
04/04/2016	A207	Introduction to LAB		
06/04/2016		Classes suspended	Three+ weeks to prepare lab activity	
11/04/2016	Mlab	Malware Lab: exploit kits		
13/04/2016	A207	Governmental & surveillance attacks		
18/04/2016	A207	Privacy in networks		
20/04/2016	Mlab	Student laboratories		
25/04/2016		Liberazione		
27/04/2016	Mlab	Student laboratories		
02/05/2016	Mlab	Student laboratories		
04/05/2016	Mlab	Student laboratories		
09/05/2016	Mlab	Student laboratories	Every session must be **booked and attended** by all students. Empty slots count as no class, but **all groups must present** before end of semester.	
11/05/2016	Mlab	Student laboratories		
16/05/2016	Mlab	Student laboratories		
18/05/2016	Mlab	Student laboratories		
23/05/2016	Mlab	Student laboratories		
25/05/2016	Mlab	Student laboratories		
30/05/2016	Mlab	Student laboratories (if needed)		
01/06/2016	Mlab	Student laboratories (if needed)		

More on the laboratory part

- Students that want to do the lab project must form groups by the 23rd of March
- All students will have at a minimum 3 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 Bro
- 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 should come

Appointments with the lecturer

- Fixed 1 hour slot every Wednesday after class
  - Questions on the course
  - Feedback on the assignments
- Book your time by email
  - luca.allodi@unitn.it
- If I am not available we will arrange a different time

The class' website

- Securitylab website for slides and material (will be online later today)
  - https://securitylab.disi.unitn.it/
  - Look for the 2015/16 Network Security course
- Announcements and assignments on Google Classroom
- **classroom.google.com**
  - Access with your UNITN credentials
  - Access class with code

9ulscl

- 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