Network Security (CS6903)

Bheemarjuna Reddy Tamma
Dept. of CSE, IIT Hyderabad

Who am I?

- Brief BIO
  - Professor in CSE Dept
  - Research Interests
    - Converged Cloud Radio Access Networks (5G/Wi-Fi)
    - Softwarization and Cloudification of Networks (SDN/NFV)
    - Internet of Things (IoT), V2X Green ICT
    - Mobile Edge Computing, Network Security
  - Teaching Interests
    - Computer Networks
    - Wireless Networks & Security
    - Operating Systems
    - Computer & Network Security
  - Administration
    - Chair of Computer Center (CC)
      - Campus networking, ICT services and policies, Data center, Office automation, etc

IIT Hyderabad

Course Instructors

Bheemarjuna Reddy Tamma

Kotaro Kataoka

Antony Franklin

Praveen Tammana

IIT Hyderabad

Objectives of the course

- A solid foundation of network security concepts
- Security mindset: how to think like attacker or security expert?
- Understanding how things work/break and how to fix them
- To learn how to monitor and analyze network traffic and protocols for detecting various types of vulnerabilities

PREREQUISITES

- Computer Networks (at least CN-1)
- Proficiency in C/C++/Python
- Familiarity with Linux environment
- Socket programming and shell scripting

Syllabus

- Introduction to network security
- Network-based threats and attacks
- A brief overview of Cryptography & PKI
- Network Authentication & Access Control
- PGP, IPSec, SSL/TLS, Tor Protocols
- TCP/IP vulnerabilities and DNS attacks
- Routing security
- IDS, Firewalls
- Email Security & Phishing
- Botnets, DDoS attacks
- Web/IoT Security
- (Differential) Privacy
- Cyber Crime, Laws, Ethics

ADMINISTRATION

- Course management through Google Classroom
  - Register for CS6903 at https://classroom.google.com/u/0/c/MjUxODgyMTA0NzYw by using **code:** cefbz5o
  - Slides, Assignments, URLs, News, Reading material, discussions posted here
- Teaching Slot:
  - P slot: MON @ 2:30PM and THU @ 4PM
- Teaching Assistants (TAs)
  - Ch Venkatarami Reddy <cs17resch01007>
  - Amalapuram Suresh <cs19resch11001>
  - Nandi Srinivas <cs19mtech11016>

IIT Hyderabad

Tentative Grading Policy

- Quizzes (online), GC queries: 35%
- Assignments/term project: 65%
  - Homework assignments
    - Written/Programming
  - Wireshark assignments
  - Term project/Hackathon

IIT Hyderabad

Assignments/Projects: Group Policy

- 1-2 students per group!
- Deliverables for wirshark asg
  - Legible report (NO copy-paste from other sources)
- Deliverables for programming asg/project
  - Design document/report, README, Code files, test files in a tar ball on GC

Collaboration and Seeking help

- Communicate with Group members
  - Divide and Conquer
  - Pose queries on GC discussion forum to seek help (not solutions) from other teams, TAs
  - Document each member's work → Assignment/Project report

- Engage with TAs
  - Discuss the problems being faced
  - Explain your methodology adapted for the project
  - Explain each member's responsibilities

IIT Hyderabad

Academic Honor Code

- Submitted work should be your own
- Acceptable collaboration:
  - Clarify problem, syntax doubts, debugging strategy
- Dishonesty has no place in any community
  - May NOT be in possession of some other Group's project
  - May NOT copy code from another group or Internet!
  - May NOT copy in lab and term exams
  - May NOT do your share of assignment work
- Penalty
  - If found guilty of copying assignments (high similarity in submitted assignments), both copy-er and copy-ee will get 0 Marks
  - Serious cases like stealing others work/cheating in lab and term exams → FR Grade

IIT Hyderabad

Dept anti-plagiarism policy: http://cse.iith.ac.in/?q=node/254

Ethics

- In this course, you will learn how to attack computer networking systems in a sandbox environment
- We learn attacks because it is needed to understand how to defend them!!
- You have an obligation to use this knowledge ethically
  - You do not attack others!
    - In addition to unethical, it may be a crime
    - Many good legitimate hacking challenges
      - http://overthewire.org/wargames/ (wargames)
      - https://challenges.re/ (reverse engineering challenges)
      - https://ctftime.org/ctfs (Capture the Flag competitions)

Reference Books/Material

- *Network Security: Private Communication in a Public World*, Kaufman, Perlman, and Speciner. *Second Edition*, Pearson, 2016
- *Cryptography and Network Security*, William Stallings, Pearson, 7th Edition, 2016, William Stallings
- *Security Engineering*, Ross Anderson, 2nd Edition (free online)
- *Computer Networking: A Top Down Approach* by James Kurose & Keith Ross, 7th Edition, Pearson, 2016.
- *Attacking Network Protocols*, James Forshaw, 2017
- Google Classroom page → articles, videos, news, etc