CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

An appeal

- Punctuality!!
- Participation

- Please Keep your notebook and pen with you

Why this 'Computer Security' course is?

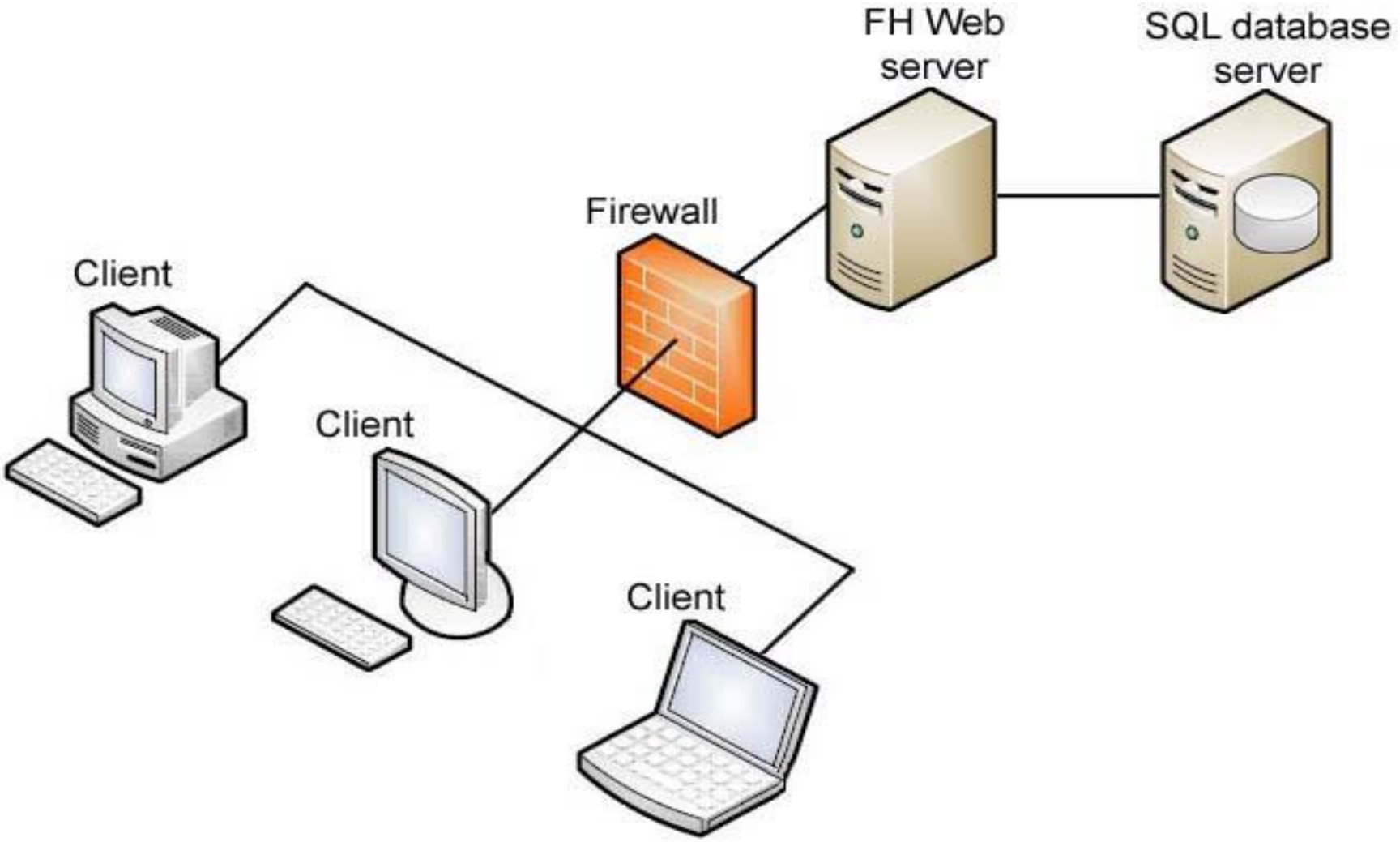
- Can one complete a Civil Engineering degree without learning anything about safety of the infrastructure (civil)?

You can complete a Computer Science degree without learning anything about critical infrastructure, security and safety!!!!

Course Objective

- Goal:
  - Primary goal is to be able to identify security and privacy issues in various aspects of computing, including:
    - Programs
    - Operating systems
    - Networks
    - Applications and Databases
- Secondarily, to be able to use this ability to design systems that are more protective of security and privacy.
- NB.: Familiarity with CS 341 Operating Systems and CS 101 Programming in C, is desirable

Foundation of Computer Security



Ex.: Web Server Application

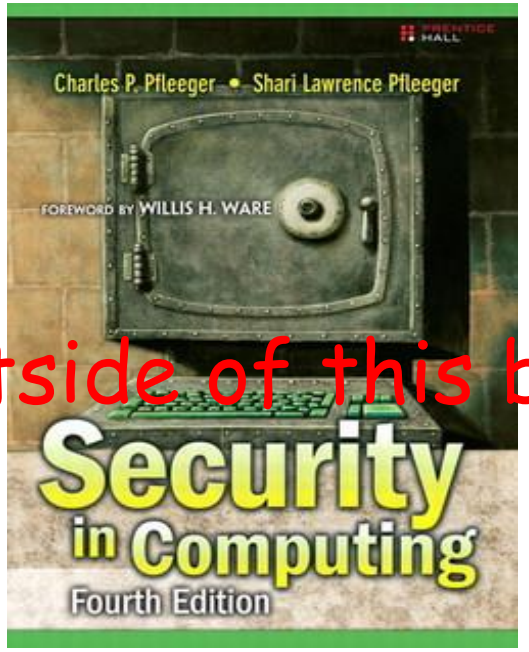
Syllabus

Familiarity with CS 341 Operating Systems and CS 101 Programming in C, is desirable

- Introduction to Computer Security and Privacy : security and privacy; types of threats and attacks; methods of defense
- Program Security: Secure programs; nonmalicious program errors; malicious code; controls against program threats
- Operating System Security: Methods of protection; access control; user authentication
- Network Security: Network threats; firewalls, intrusion detection systems
- Application Security and Privacy: Basics of cryptography; security and privacy for Internet applications (email, instant messaging, web browsing); privacy-enhancing technologies. Database Security and Privacy: Security and privacy requirements; reliability, integrity, and privacy; inference;

Required textbook

Security in Computing, 4th edition
Charles P. Pfleeger and Shari Lawrence Pfleeger
Prentice-Hall, 2007 or later



I would follow outside of this book most often. So please be regular to all the classes.

Slides & Assignments will be uploaded/ posted.

Course mechanics

- Course webpage

  Googledocs in our group

- Evaluation
  - Assignments, Quiz-tests. Term Project (35-30%)
  - Midterm (25%)
  - Final (35%)
  - Class participation/ Attendance 5-10%

- Attendance: Full attendance is expected being an Elective course

- Your participation in the class has major value

For Discussion

- You can reach me
  - som@iitp.ac.in
  - Text/call/ WhatsApp:8084717331
- T.A.:
  - Mr. Harsh
    - "harsh 1921cs01" <harsh_1921cs01@iitp.ac.in>;
  - Mr. Narendra

Course Outcomes

- Will make you to realize\ understand
  - think like an attacker
  - Be informed of the issues.
    - Because many developers don't even consider security in software.
  - the tradeoffs
- This Course Is NOT
  - Forensic and anti-forensics
  - Social engineering
  - Reverse engineering
  - Security management
  - Hack all things
  - Privacy
  - Cryptographic Algorithms

Pl note

You are not to test the security of, break into, compromise, or otherwise attack, any system or network

without the express consent of the owner

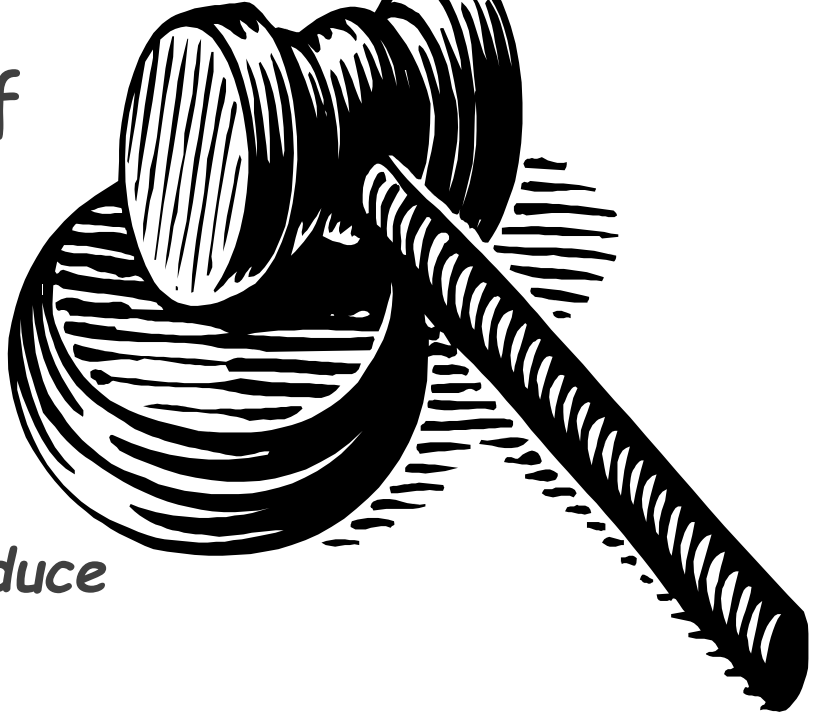
Caution!!!!

- Kevin Mitnick
  - First hacker on FBI's Most Wanted list
  - Hacked into many networks
    - including FBI
  - Stole intellectual property
    - including 20K credit card numbers
  - In 1995, caught 2nd time
    - served five years in prison

Recent Indian context

- 2014:
  - Amit Vikram Tiwari, Global hacker arrested
  - He was nabbed in 2003 as well.
- compromises 950 foreign email accounts and 171 Indian;
-
- 2019:
  - 33-year-old Indian man has been sentenced to three months in prison followed by deportation for hacking 15 websites,
- May 2020
  - Facebook hackers arrested by Azamgarh Police

Whoever without permission of the owner of the computer :



- ***Secures Access;***
- ***Downloads, Copies or extracts any data, computer database or any information;***
- ***Introduce or causes to be introduce any Virus or Contaminant;***
- ***Disrupts or causes disruption;***
- ***Tampering with or Manipulating any Computer, Computer System, or Computer Network;***

Shall be liable to pay damages by way of compensation.

Cyber Law is represented by Indian IT ACT 2008

Computer Security

- **What is Computer Security?**
  - Computer Security is the protection of computing systems and the data that they store or access.

- **Why is Computer Security Important?**
  - Computer Security allows the organization to carry out its mission by Protecting personal data and sensitive information

Why Computer Security?

- The Internet is a dangerous place
  - We are constantly being scanned for vulnerable systems
    - new unpatched systems will be exploited within minutes.
- Lab (Govt. or Industry) is an attractive target
  - High network bandwidth is useful for attackers who take over lab computers
  - Publicity value of compromising a .gov site
  - Attackers may not realize we have no information useful to them

Source of Danger

- We need to protect
  - Our data
  - Our ability to use our computers (denial of service attacks)
  - Our reputation with Congress and the general public
- Major sources of danger
  - Running malicious code on your machine due to system or application vulnerabilities or improper user actions
  - Carrying infected machines (laptops) in from off site

Defining Security

- Security : *Ability to avoid being harmed by any risk, danger or threat* (Cambridge dictionary)

- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary with specific capabilities

- Security is achieving some goals in presence of Adversary

Thanks