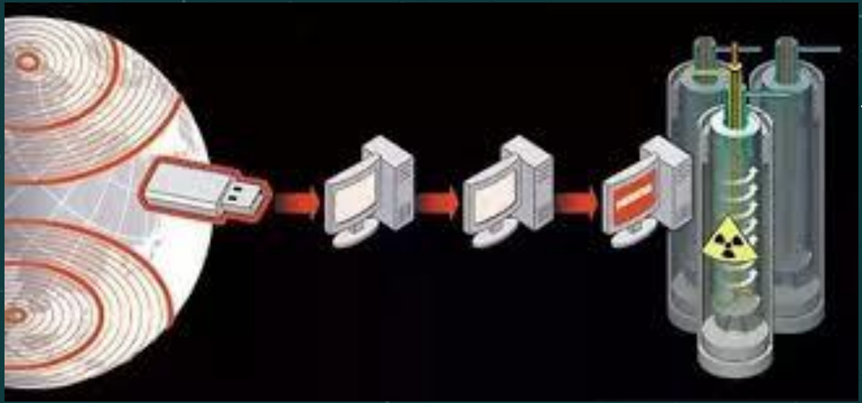
# Computer Security Concepts

Information Security – Lecture 01

Aadil Zia Khan

# Stuxnet - When Countries go Rogue



- Ruined almost one-fifth of Iran's nuclear centrifuges by changing the centrifuges' rotor speed
- Targeted machines using the Microsoft Windows operating system and then searched for the Siemens Step7 software
- Considered to be a cyberweapon built jointly by the United States and Israel

# Recent Data Breaches

In 2019, a Pakistani hacker, Gnosticplayers, hacked into Zynga's database and gained access to the 218 million accounts

Names, dates of birth, email addresses and passwords, and security questions and answers of 3 billion Yahoo users were leaked in 2013

165 million user Linkedin accounts had their passwords stolen and sold for around 2000$

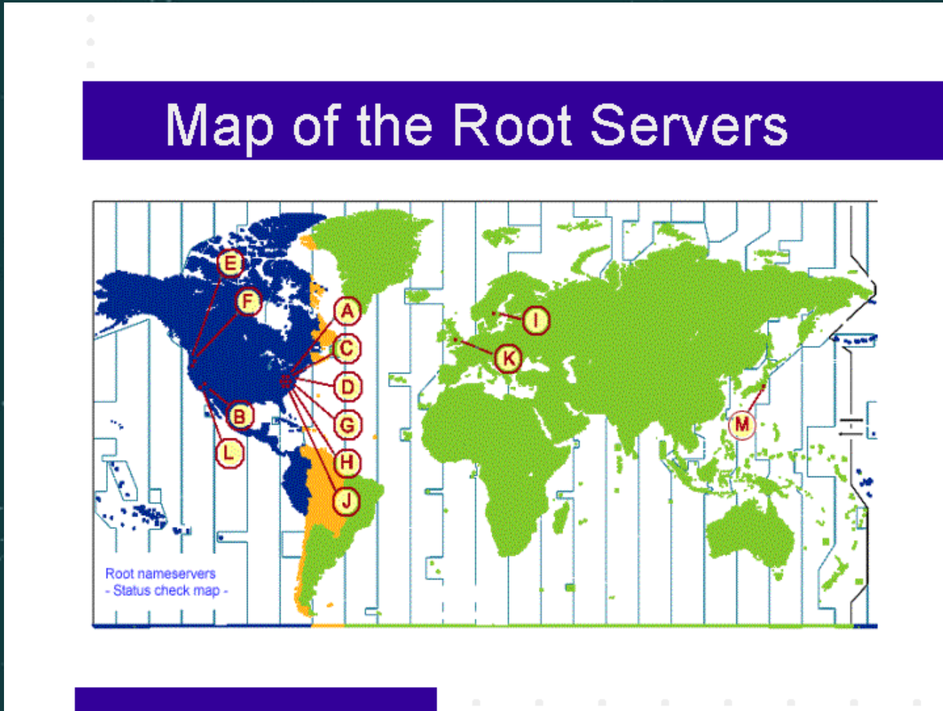
# pkBrain - The First PC Virus

- Basit and Amjad Farooq Alvi, who ran a computer store in Pakistan were tired of customers making illegal copies of their software
- Made **pkBrain** in 1986 - the first PC virus
- It infected 5.2" floppy disks - the virus slowed down the floppy disk drive and made some memory unavailable to DOS

# Can we Break the Internet ?

- In 2002, a cyber attack aimed at all 13 domain name system's root servers in the US almost brought the Internet to its knees

- It was a DDoS attack lasting an hour – so much malicious traffic was generated that servers were overwhelmed and unable to respond to valid requests



Map of the Root Servers

# Course Outline

- Introduction
- Cryptography
- Authentication and Access Control
- Software and OS Security
- Web Security and Internet Security Protocols
- Denial of Service
- Intrusion Detection and Firewalls
- IoT Security (if time permits)
- Blockchain (if time permits)

# Teaching Style

- Interactive
- In class practice questions
- Application of concepts

If you do not understand something – in-class queries and visits to my office are encouraged

# Grade Distribution (Tentative)

Will be decided later – once the covid status is clear

# LMS and Zoom

You will be added to the course page on LMS - visit it daily for

- Important announcements
- Assignments
- Course related material (slides, reading material, outlines, office hours)

Classes will be conducted simultaneously in the room as well as on Zoom

- Follow the university policy regarding physical/online attendance

# Stresses / Problems

In case there is any issue talk to the instructor well in time

- Problems at home
- Struggling with coursework/assignment
- Need to use phone during the class/exam

# Antisocial Behavior

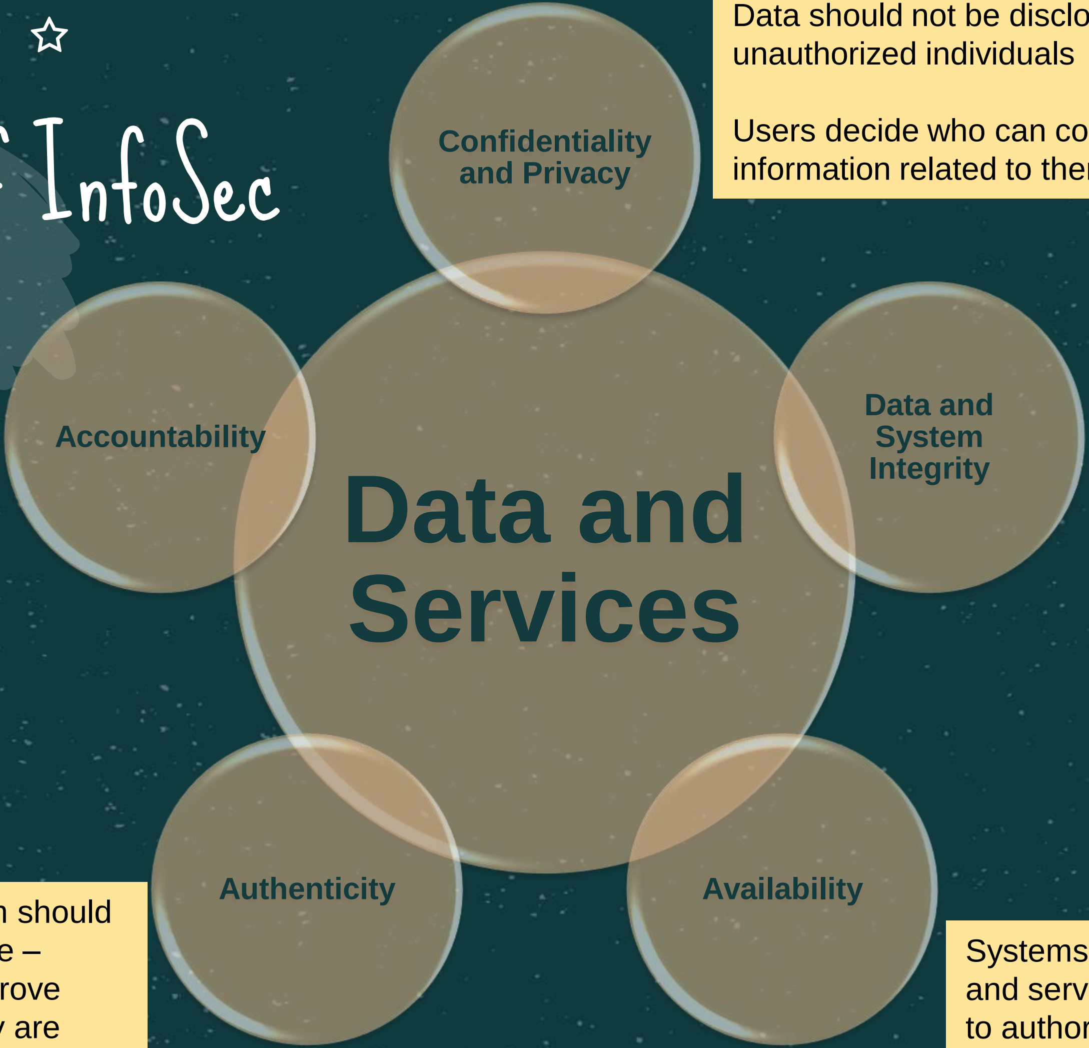
Penalty ranging from zero in the grading instrument to F in course

- Plagiarism
- Mobile phone usage during class/exam
- Disturbing other students
- Bullying / Harassment

# Why Study this Course

- For motivation
- Get an idea of what lies ahead
- To ease the transition into future courses
- Hands on practice of various tools that would be needed in the future

# Pillars of InfoSec



Data should not be disclosed to unauthorized individuals

Users decide who can collect what information related to them

Data should be accurate, complete, and consistent

Source should not be able to deny that the data was from it (principle of non repudiation)

System should not be tampered with by unauthorized personnel and it should verifiably work properly

Systems should work promptly and service should not denied to authorized users

Input arriving at the system should come from a trusted source – source should be able to prove they are who they say they are

System should be able to trace a security breach to the responsible party

Systems must keep records of their activities to trace security breaches or to aid in disputes

# Security Principles in a Medical Application

| Confidentiality | Integrity | Availability | Authenticity | Accountability |
|---|---|---|---|---|
| • Medical reports should not be visible to everyone | • Medical reports should not be falsified | • Medical reports should be accessible to the medical practitioners whenever needed | • Doctor should be able to ascertain the medical reports came from the lab | • In case the medical report gets messed up, their should be a log of who worked on the reports |

# Impact of a Security Breach

- Low
  - Results will have a minor impact – e.g., student enrollment information leak
- Medium
  - Result on significant damage but still bearable to some extent – e.g., minor loss in the stock market due to system becoming inaccessible which doesn't end up bankrupting a company
- High
  - Results will be catastrophic – e.g., nuclear passcodes getting exposed, nurse switching patient's lab reports

# InfoSec Challenges - Why is it so Difficult?

- System designer addresses all known threats – and thinks of all potential threats
  - Hacker creates a new threat that no one had previously thought of
- Too many layers need to be secured
  - E.g., physical device, network links, OS/software
- Sometimes passwords/keys need to be shared over an insecure medium
  - Capture that and you have completely compromised the security
- Strong security could make the system complex – or difficult to use
  - E.g., imagine UMT system administrator asking you to change password everyday

Security should be a design principle – not an afterthought