EE4758/IM3003 COMPUTER/INFORMATION SECURITY
TUTORIAL NO. 4

1. **What are the two aspects of computer security and explain why computer security strategies that are technology-centric or policy-centric always fail. Also suggest ways to overcome this major problem?**

   ➔ Technological (Hardware, Software, Network)

   ➔ Managerial (policies, procedures)

- **TECHNICAL**

  ➔ Main focus is on developing **technical expertise** and technologies for computer security.

- **MANAGERIAL**

  ➔ The focus is on developing security **policies** and **procedures**.

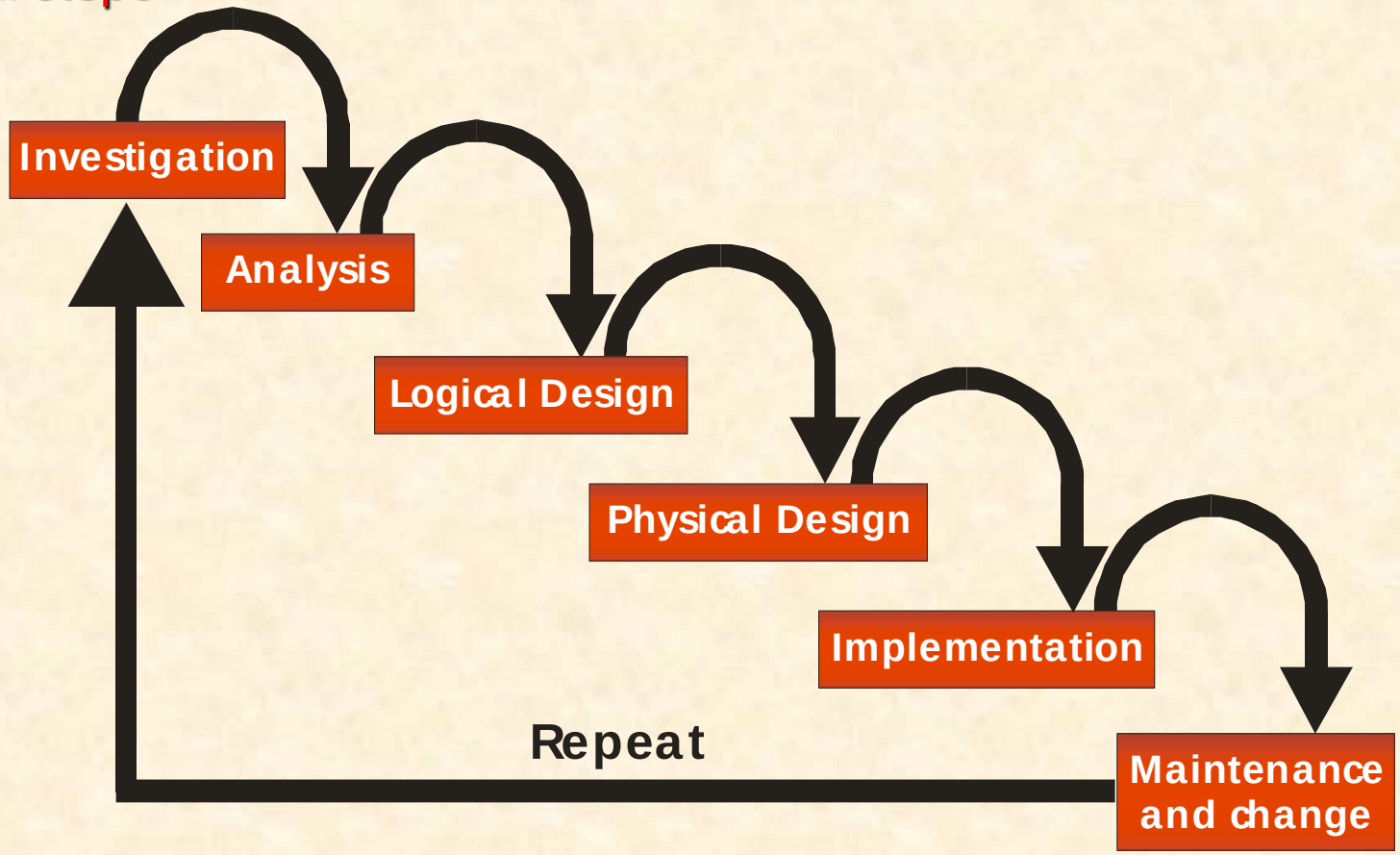
- Basically these **two groups** of people in any organization **have different roles and functions.**
- The problem arises because both groups **don't understand** and **appreciate** each other's work.
- Without each **other's cooperation**, they will not succeed.

COMPUTER SECURITY DEFENCE MODEL

Tier 1	Senior management commitment and support
Tier 2	Acceptable-use policies and other statements of practice
Tier 3	Secure-use procedures
Tier 4	Hardware, software, and network security tools

- **Technology-centric** strategies are **weak without** strong **policies** and **practices.**
- **Policy-centric** strategies are **ineffective without technology** to monitor and enforce them.
- **What is needed** is a comprehensive multi faceted approach based on:
  - ➔Senior management support
  - ➔Strong and sensible policies
  - ➔Practical procedures.
  - ➔Modern Security Technologies
- Because **all** four **play** a **vital role** in the proper execution of a computer security program.
- **Management is responsible**
- **Information security is**
  - ➔A management issue
  - ➔A people issue

2. Assume that you have been appointed a security consultant in a start-up company which is starting branches in several countries. The higher management is not very technical, however they do know the importance of computer security and are all geared up to support whatever measure you are willing to take. Thus, describe various steps you will take to set-up a proper security system for the organization and what will be the two most important initial steps.



- **First step** in security planning: **Identification**
- **Identify** what the organization needs to protect--and to protect against.
  - ➔ Identify the types of threat facing an organization's information systems.
- **Next step** in security planning is **Understand vulnerabilities**
- Vulnerabilities normally exist for **two key reasons**:
  1. **Human error**, such as using poor passwords or participating in chat rooms from business email accounts.
  2. **Complexity of software** that results in miss-configuration, and programming errors.

3. In the above example, if the top management was not keen on computer security, would you still be able to design, implement and manage the security system? If not what would you do to convince the higher management that the security should be taken seriously.

- Well one can design and implement the security system, but without proper policies and enforcement, it will not be effective.
- To convince the top management, one needs to make them realize the extent of the problem and what is at risk in their own organization.
- **ASSETS AT RISK**
  - ➔ Data assets
  - ➔ Knowledge assets
  - ➔ Software assets
  - ➔ Physical assets
  - ➔ Monetary or financial assets
  - ➔ Employee assets
  - ➔ Customer and partner assets
  - ➔ Goodwill

- Employees and staff cannot be expected to change their behavior if they do not observe respect for security by their superiors.
- Management must be informed of the various kinds of threats facing the organization
- **How to get management's attention?**
  - ➔ **News that gets attention:**
    - 4,000 ecommerce Websites attacked each week!
    - Yahoo! suffered a $1 billion loss in share price directly following a DOS attack.
    - 39% of companies had downtime lasting over 8 hours from DOS attacks.
    - Theft of intellectual property is costing U.S. businesses more than $250 billion annually, according to the American Society of Industrial Security (ASIS). Much of this property drain is conducted electronically.

4. Your company installs a face recognition system for door access. Initially its FRR is much worse than the vendor's claims, however the system's FRR increases over time. What might be causing this?

- An FRR worse than vendor claims is not that unusual.
- Vendor claims are likely exaggerated as they base their claims upon ideal recognition conditions (perfect lighting, un-obscured view of the face, small number of templates to compare with).
- In reality, the company's implementation of the face recognition system is under conditions far from ideal, thus the lower than expected FRR.
- Over time, the number of templates in the system for comparison will surely increase.
- Given a static false rejection probability, the FRR will increase with the number of templates.
- In addition, people's faces will change over time.

5. Can someone access your computer by guessing your password and are there additional options that would make guessing passwords faster?

- Probably not. It's highly unlikely that someone will gain access to your computer by guessing your password.
- There are just too many passwords to guess.
- Most accounts are locked out (or timed out) if someone enters the incorrect password more than three or four times.
- There are much easier ways to gain access to your computer i.e. using password cracker software and launching dictionary attacks.
- Yes, there are certain patterns that people follow when creating passwords and that may make guessing/cracking a password faster/easier.
- Many people put a number either before or after their password. Crackers know this.
  - ➔ They can set options that will force the cracker program to try variations based on these known patterns.
  - ➔ This increases the probability of cracking passwords faster.
- Also using names of famous people (film stars, authors etc.) or some words (e.g. iloveyou, mybestfriend etc.) are easy to crack using dictionary attack.
- Short passwords are another easy option for cracking it fast.

QUIZ

A. What additional security technologies would be useful to ensure the authenticity of the actual operator of a client computer?

i. Biometrics
ii. Firewalls
iii. IDS
iv. None of the above

Answer: Biometrics

A. What should an employee do if she believes her password has been revealed to another party?

i. If it is a trusted employee or friend, just ignore it.
ii. Change your own password immediately.
iii. Notify the IT department.
iv. Ignore it.

Answer: Change your own password immediately.

C. Statements made by management that lays out the organization's position on an issue are called _____.

I. Policies
II. Procedures
III. Standards
IV. Guidelines

- **Answer: Policies**

D. When creating a password, users tend to use

i. All capital letters
ii. Passwords that is too long
iii. Names of family, pets, or teams
iv. Numbers only

- **Answer: Names of family, pets, or teams**

E. A good security practice is to choose one good password and use it for all of your various accounts.

i. TRUE/FALSE

- **Answer: FALSE**