CSC 519 Information Security

LECTURE 8: Administering security

Dr. Esam A. Alwagait
alwagait@ksu.edu.sa

outline: Administering security

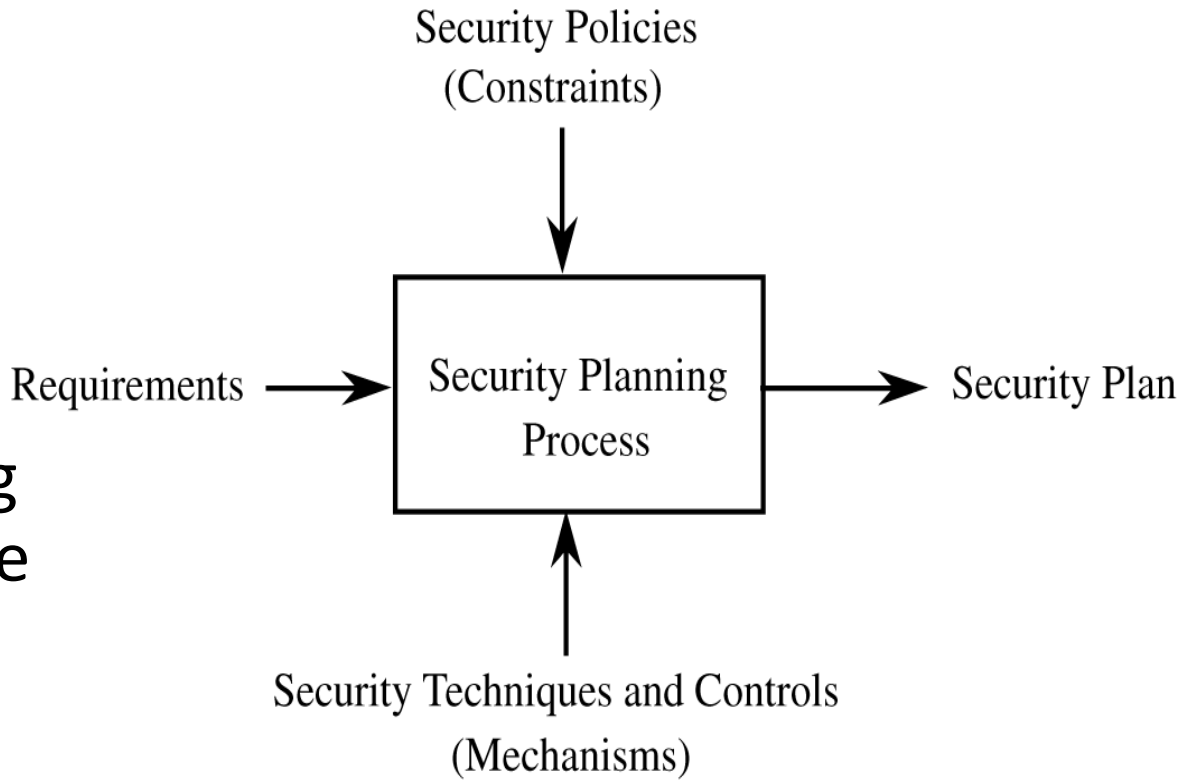
- Security planning
- Risk analysis
- Security policies
- Physical security

Overview

- So far we have learned how to achieve security, protecting programs, operating systems, databases, and networks, using technology (technical controls)
- While this is essential, but not all of security and privacy issues are addressed by technology
- Security controls are combination of
  - Technical controls
  - Administrative controls
  - Physical controls

Security planning

- Every organization using computing resources should perform thorough and effective security planning
- A security plan is a document that describes how an organization will address its security needs, specifying its security goals, and how to achieve them
- The plan should be reviewed and revised periodically



Contents of a security plan

- A security plan identifies and organizes the security activities for a computing system
- The plan is both a description of the current situation and a plan for improvement
- Every security plan must address seven issues:
  - Policy: A security policy is a high-level statement of purpose and intent, specifying goals, responsibility, and commitment
  - current state: describing the status of security at the time of the plan, e.g., current assets, vulnerabilities, responsibilities.
  - Requirements: specifying the needs that the organization has, e.g., who is allowed/not allowed, what logs should be kept, etc.
  - Recommended controls: mapping controls to the vulnerabilities identified in the current state and requirements in the light of the security policy
  - Accountability: describing who is responsible for each security activity in the case of failure, e.g., specifying responsibilities for desktop users, DB admins, network admins, CSO, CIO, etc.
  - Timetable: identifying when different security functions are to be done, e.g., procurement of HW, installation, operations, and maintenance, etc.
  - Continuing attention: specifying a structure for periodically updating the security plan, as the state of the world, technology, vulnerabilities is not static!

Risk analysis

- A risk is a potential problem that the system or its users may experience
- Risk analysis is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause
- Three strategies for dealing with risk
  - Risk avoidance: by changing requirements for security or other system characteristics
  - Risk transference: by allocating the risk to other systems, people, organizations, or assets; or by buying insurance to cover any financial loss should the risk become a reality
  - Risk acceptance: by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs

Risk analysis

- Risk analysis usually comprises the following steps:
  - Identify assets
    - what we need to protect
  - Determine vulnerabilities
    - predict what damage might occur to the assets and from what sources
  - Estimate likelihood of exploitation
    - how often each exposure is likely to be exploited
  - Compute expected loss
    - determine the likely loss if the exploitation does indeed occur
  - Survey applicable controls
    - see which controls address the risks identified in previous steps
  - Project savings due to control
    - determine whether the costs outweigh the benefits of preventing or mitigating the risks

Security policies

- A security policy is a high-level management document to inform all users of the goals of and constraints on using a system
- A security policy must answer three questions: who can access which resources in what manner?
- Characteristics of a good security policy
  - Coverage: a security policy must be comprehensive, and general enough to apply to new cases
  - Durability: a security policy must grow and adapt well
  - Realism: it must be possible to implement the stated security requirements with existing technology
  - Usefulness: it must be clear, direct, and understood
- Examples
  - "Each security officer shall . . . perform a risk assessment to identify and document specific . . . assets, . . . threats, . . . and vulnerability . . ."
  - "Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls"

Physical security

- There are many threats to security that involve human or natural disasters
  - Humans:
    - Thieves, vandals, etc.
  - Natural:
    - Fire, flood, hurricanes, storms, etc.
- Physical security is the term used to describe protection needed outside the computer system
- Typical physical security controls include guards, locks, CCTVs, backups, and fences to deter direct attacks
- The primary physical controls are strength and duplication
  - Strength means overlapping controls implementing a defense-in-depth approach so that if one control fails, the next one will protect
  - Duplication means having redundant copies of data, spare hardware components, etc.

The big picture of security and privacy

- Now, we know how to protect components of a computing environment:
  - Programs
  - Operating systems
  - Databases
  - Networks
  - Physical assets
- With
  - Technical controls
  - Administrative controls
  - Physical controls