ECS 235B Module 13
Security Policies
Security Policy

• Policy partitions system states into:
  • Authorized (secure)
    • These are states the system can enter
  • Unauthorized (nonsecure)
    • If the system enters any of these states, it’s a security violation

• Secure system
  • Starts in authorized state
  • Never enters unauthorized state
Confidentiality

• $X$ set of entities, $I$ information
• $I$ has the confidentiality property with respect to $X$ if no $x \in X$ can obtain information from $I$
• $I$ can be disclosed to others
• Example:
  • $X$ set of students
  • $I$ final exam answer key
  • $I$ is confidential with respect to $X$ if students cannot obtain final exam answer key
Integrity

• $X$ set of entities, $I$ information

• $I$ has the *integrity* property with respect to $X$ if all $x \in X$ trust information in $I$

• Types of integrity:
  • Trust $I$, its conveyance and protection (data integrity)
  • $I$ information about origin of something or an identity (origin integrity, authentication)
  • $I$ resource: means resource functions as it should (assurance)
Availability

• $X$ set of entities, $I$ resource

• $I$ has the availability property with respect to $X$ if all $x \in X$ can access $I$

• Types of availability:
  • Traditional: $x$ gets access or not
  • Quality of service: promised a level of access (for example, a specific level of bandwidth); $x$ meets it or not, even though some access is achieved
Policy Models

• Abstract description of a policy or class of policies
• Focus on points of interest in policies
  • Security levels in multilevel security models
  • Separation of duty in Clark-Wilson model
  • Conflict of interest in Chinese Wall model
Mechanisms

• Entity or procedure that enforces some part of the security policy
  • Access controls (like bits to prevent someone from reading a homework file)
  • Disallowing people from bringing CDs and floppy disks into a computer facility to control what is placed on systems
Question

• Policy disallows cheating
  • Includes copying homework, with or without permission
• CS class has students do homework on computer
• Anne forgets to read-protect her homework file
• Bill copies it
• Who breached security?
  • Anne, Bill, or both?
Answer Part 1

• Bill clearly breached security
  • Policy forbids copying homework assignment
  • Bill did it
  • System entered unauthorized state (Bill having a copy of Anne’s assignment)

• If not explicit in computer security policy, certainly implicit
  • Not credible that a unit of the university allows something that the university as a whole forbids, unless the unit explicitly says so
Answer Part 2

• Anne didn’t protect her homework
  • Not required by security policy

• She didn’t breach security

• If policy said students had to read-protect homework files, then Anne did breach security
  • She didn’t do this
Types of Security Policies

• Military (governmental) security policy
  • Policy primarily protecting confidentiality

• Commercial security policy
  • Policy primarily protecting integrity

• Confidentiality policy
  • Policy protecting only confidentiality

• Integrity policy
  • Policy protecting only integrity
Integrity and Transactions

• Begin in consistent state
  • “Consistent” defined by specification

• Perform series of actions (*transaction*)
  • Actions cannot be interrupted
  • If actions complete, system in consistent state
  • If actions do not complete, system reverts to a consistent state
Types of Access Control

• Discretionary Access Control (DAC, IBAC)
  • Individual user sets access control mechanism to allow or deny access to an object

• Mandatory Access Control (MAC)
  • System mechanism controls access to object, and individual cannot alter that access

• Originator Controlled Access Control (ORCON, ORGCON)
  • Originator (creator) of information controls who can access information