Chapter 4: Security Policies

- Overview
- Policies
- Trust
- Example Policy

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

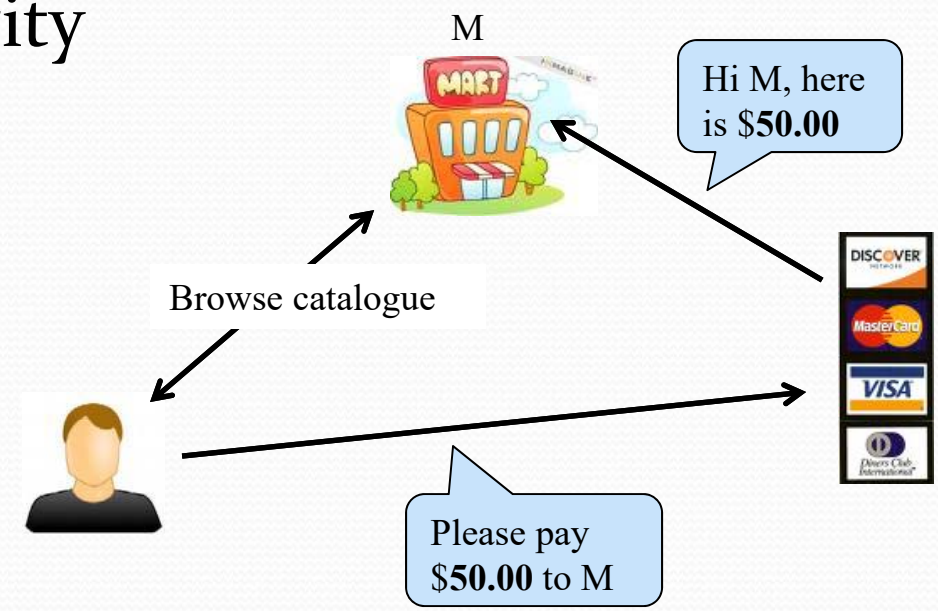
- *X* set of entities, *I* information
- *I* has *confidentiality* property with respect to *X* if no $x \in X$ can obtain information from *I*
- *I* can be disclosed to others
- Example:
  - *X:* set of students
  - *I:* home work answer key
  - *I* is confidential with respect to *X* if students cannot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

Integrity

- *X* set of entities, *I* information
- *I* has *integrity* property with respect to *X* if all $x \in X$ trust information in *I*
- Types of integrity:
  - trust *I*, its transmission and storage (data integrity)

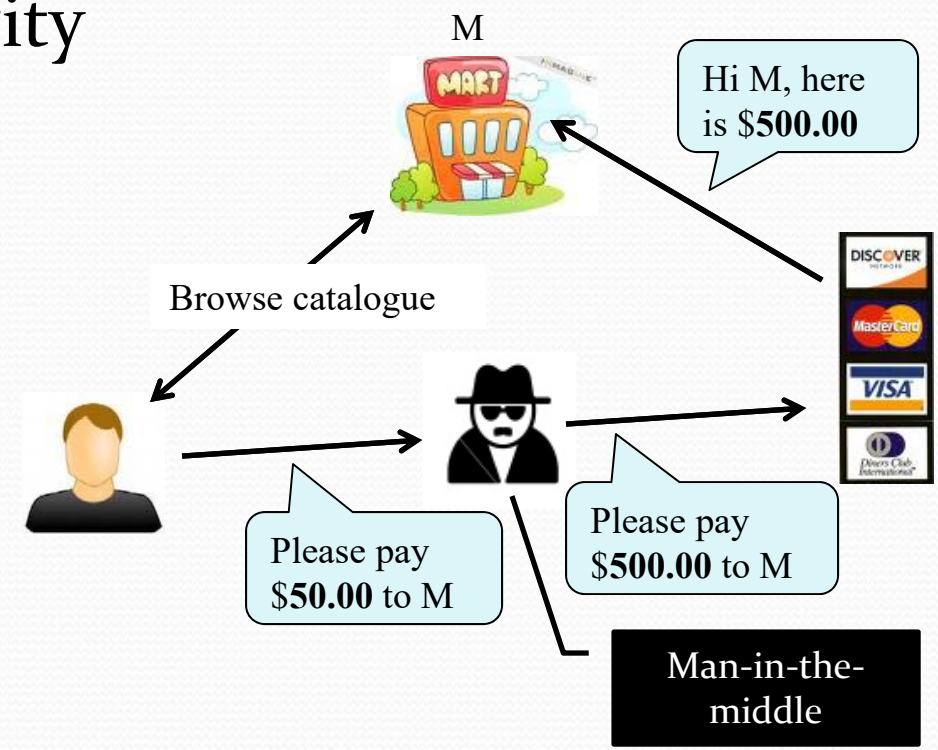
Examples: Data Integrity

- Transmission integrity
  - Online shopping



Examples: Data Integrity

- Transmission integrity
  - Online shopping



Examples: Data Integrity

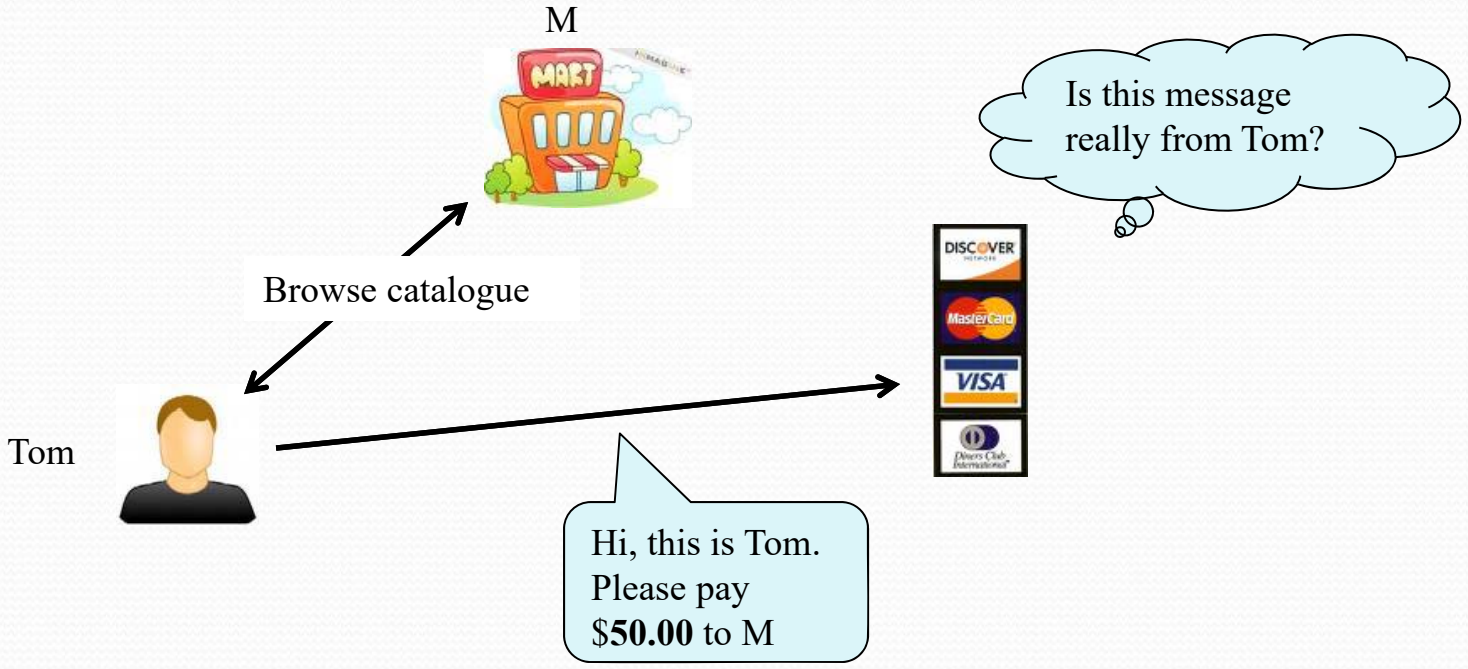
- Transmission integrity
  - Online shopping
- Storage integrity
  - Presentation slides and a cheap USB drive

Integrity

- *X* set of entities, *I* information
- *I* has *integrity* property with respect to *X* if all $x \in X$ trust information in *I*
- Types of integrity:
  - trust *I*, its transmission and storage (data integrity)
  - *I* information about origin of something or an identity (origin integrity, authentication)

Example: Authentication

- Information about origin of something or an identity (origin integrity, authentication)



Integrity

- *X* set of entities, *I* information
- *I* has *integrity* property with respect to *X* if all $x \in X$ trust information in *I*
- Types of integrity:
  - trust *I*, its transmission and storage (data integrity)
  - *I* information about origin of something or an identity (origin integrity, authentication)
  - *I* resource: means resource functions as it should (assurance)

Example: Assurance

- Definition: a resource functions as it should
- What are the resources and things that affect their assurance?
  - Network links

Example: Assurance

- Definition: a resource functions as it should
- What are the resources and things that affect their assurance?
  - Network links → transmission errors

Example: Assurance

- Definition: a resource functions as it should
- What are the resources and things that affect their assurance?
  - Network links → transmission errors
  - Applications

Example: Assurance

- Definition: a resource functions as it should
- What are the resources and things that affect their assurance?
  - Network links → transmission errors
  - Applications → Trojan horses

Example: Assurance

- Definition: a resource functions as it should
- What are the resources and things that affect their assurance?
  - Network links → transmission errors
  - Applications → Trojan horses
  - Operating systems

Example: Assurance

- Definition: a resource functions as it should
- What are the resources and things that affect their assurance?
  - Network links → transmission errors
  - Applications → Trojan horses
  - Operating systems → rootkits

Integrity

- *X* set of entities, *I* information
- *I* has *integrity* property with respect to *X* if all $x \in X$ trust information in *I*
- Types of integrity:
  - trust *I*, its transmission and storage (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 *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 (QoS): promised a level of access (for example, a specific level of bandwidth in voice over IP) and not meet it, even though some access is achieved

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

The Role of Trust

A system administrator receives and installs a security patch for her computer's operating system.

If she claims to have improved the security of her system, what does she have to trust in order to support such a claim?

The Role of Trust

1. Trusts patch came from vendor, not tampered with in transit
2. Trusts vendor tested patch thoroughly
3. Trusts vendor's test environment corresponds to local environment
4. Trusts patch is installed correctly

Trust in Formal Verification

- Gives formal mathematical proof that given input *i*, program *P* produces output *o* as specified
- Suppose a security-related program *S* formally verified to work with operating system *O*
- What are the assumptions?

Trust in Formal Methods

1. Proof has no errors
   - Bugs in automated theorem provers
2. Preconditions hold in environment in which *S* is to be used
   - Command line input
3. *S* transformed into executable *S′* whose actions follow source code
   - Compiler bugs, linker/loader/library problems
4. Hardware executes *S′* as intended
   - Hardware bugs (Intel Pentium `f00f` bug, for example)

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)
  - originator (creator) of information controls who can access information

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 cheated?
  - Anne, Bill, or both?

Answer Part 1

- Bill cheated
  - 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 read-protect her homework

Example English Policy

- Computer security policy for academic institution
  - Institution has multiple campuses, administered from central office
  - Each campus has its own administration, and unique aspects and needs
- Authorized Use Policy
- Electronic Mail Policy

Authorized Use Policy

- Intended for one campus (Davis) only
- Goals of campus computing
  - Underlying intent
- Procedural enforcement mechanisms
  - Warnings
  - Denial of computer access
  - Disciplinary action up to and including expulsion
- Written informally, aimed at user community

Electronic Mail Policy

- Systemwide, not just one campus
- Three parts
  - Summary
  - Full policy
  - Interpretation at the campus

Summary

- Warns that electronic mail not private
  - Can be read during normal system administration
  - Can be forged, altered, and forwarded
- Unusual because the policy alerts users to the threats
  - Usually, policies say how to prevent problems, but do not define the threats

Summary

- What users should and should not do
  - Think before you send
  - Be courteous, respectful of others
  - Don't interfere with others' use of email
- Personal use okay, provided overhead minimal
- Who it applies to
  - Problem is UC is quasi-governmental, so is bound by rules that private companies may not be
  - Educational mission also affects application

Full Policy

- Context
  - Does not apply to Dept. of Energy labs run by the university
  - Does not apply to printed copies of email
    - Other policies apply here
- E-mail, infrastructure are university property
  - Principles of academic freedom, freedom of speech apply
  - Access without user's permission requires approval of vice chancellor of campus or vice president of UC
  - If infeasible, must get permission retroactively

Uses of E-mail

- Anonymity allowed
  - Exception: if it violates laws or other policies
- Can't interfere with others' use of e-mail
  - No spam, letter bombs, e-mailed worms, *etc*.
- Personal e-mail allowed within limits
  - Cannot interfere with university business
  - Such e-mail may be a "university record" subject to disclosure

Security of E-mail

- University can read e-mail
  - Won't go out of its way to do so
  - Allowed for legitimate business purposes
  - Allowed to keep e-mail robust, reliable
- Archiving and retention allowed
  - May be able to recover e-mail from end system (backed up, for example)

Implementation

- Adds campus-specific requirements and procedures
  - Example: "incidental personal use" not allowed if it benefits a non-university organization
  - Allows implementation to take into account differences between campuses, such as self-governance by Academic Senate
- Procedures for inspecting, monitoring, disclosing e-mail contents
- Backups

Key Points

- Policies describe *what* is allowed
- Mechanisms control *how* policies are enforced
- Trust underlies everything