590.05 Lecture 3: Tools to Security

Xiaowei Yang

Previous lecture

- C.I.A.
  - Confidentiality
  - Integrity
  - Availability

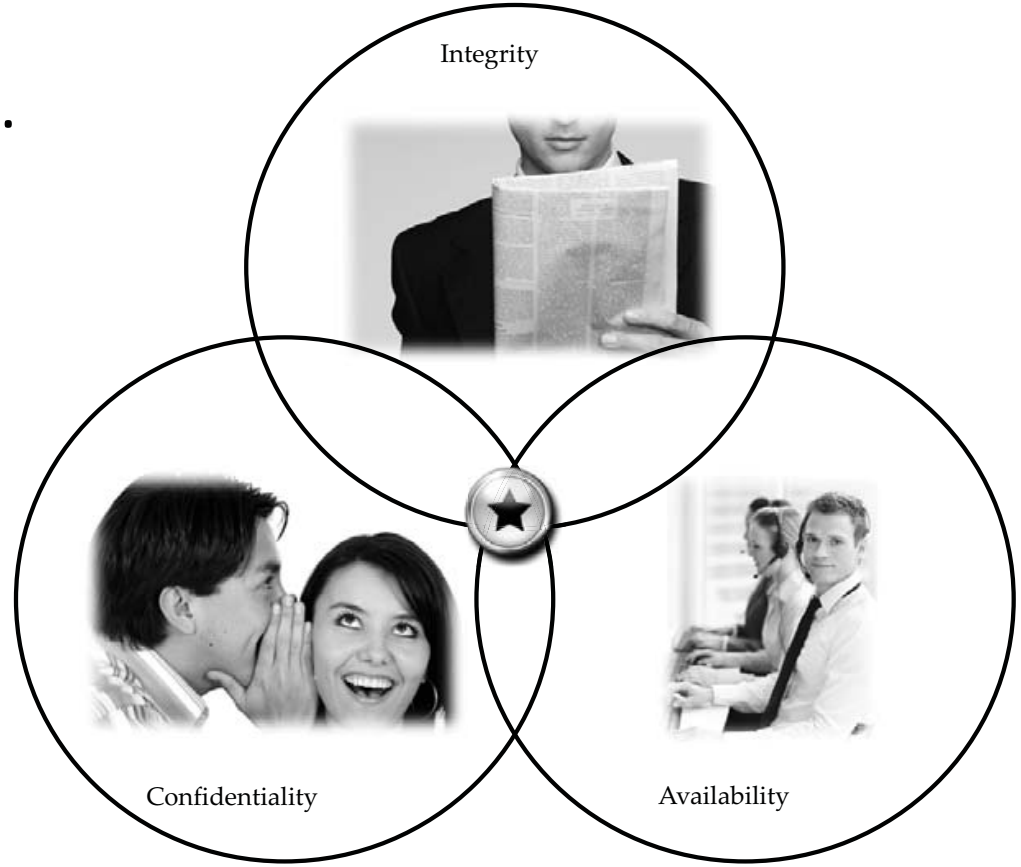
- What to trust

Today

- More security goals
- Tools to security

Security goals

- C.I.A.

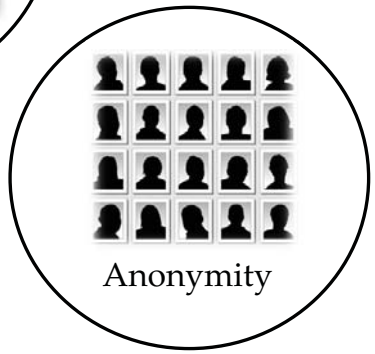


Classic goals: C.I.A.

- **Confidentiality** is the avoidance of the unauthorized disclosure of information.
  - confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.
- **Integrity:** the property that information has not be altered in an unauthorized way.
  - .
- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so.

More security goals

- A.A.A.



Assurance, Authenticity, and Anonymity

- Assurance: refers to how trust is provided and managed in computer systems
- Authenticity: the ability to determine the statements, policies, and permission issued by persons or systems are genuine, not faked
- Anonymity: certain transactions or records not to be attributable to any individual

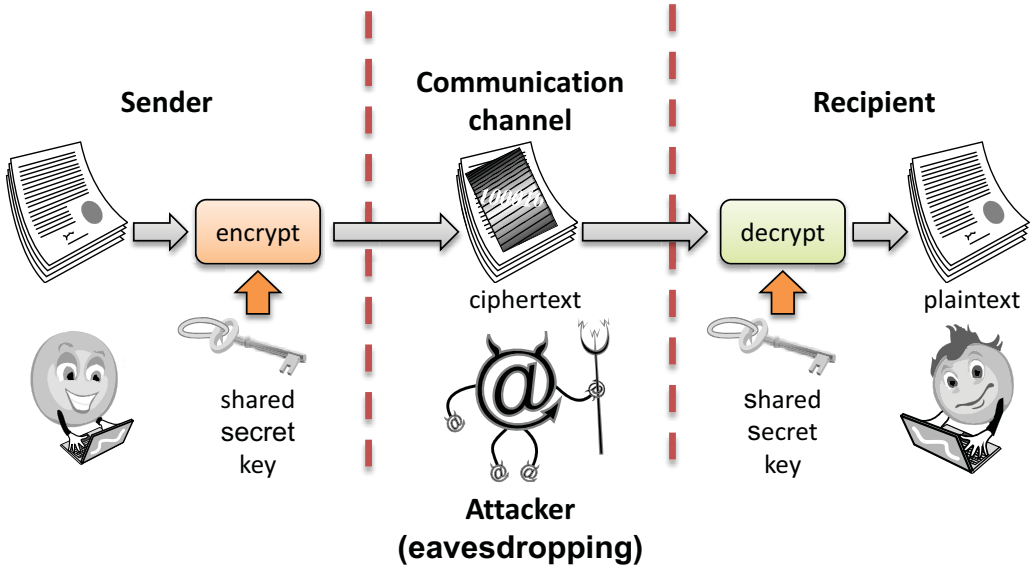
TOOLS FOR SECURITY

Tools for confidentiality

- Encryption
- Access control
- Authentication
- Authorization

Encryption

- **Encryption:** the transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (which may, in some cases, be the same as the encryption key).

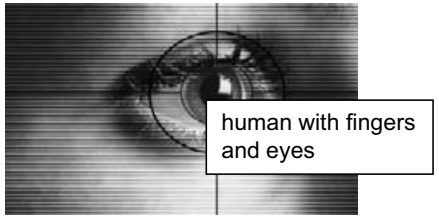


Access control

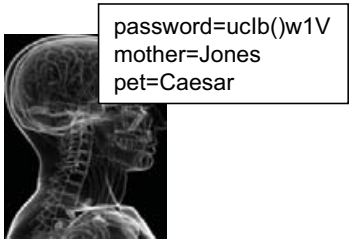
- **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a “need to know.”
  - This need to know may be determined by identity, such as a person’s name or a computer’s serial number, or by a role that a person has, such as being a manager or a computer security specialist.

Authentication

- **Authentication:** the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).



Something you are



Something you know

Something you have

- Two factor authentication

Authorization

- Authorization: the determination if a person or a system is allowed access to resources, based on an access control policy
  - Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources

Physical security

- Physical security: the establishment of physical barriers to limit access to protected computational resources
  - Such barriers include locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called **Faraday cages)** so that electromagnetic signals cannot enter or exit the enclosure.

Tools for Integrity

- **Backups:** the periodic archiving of data.
- **Checksums:** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
- **Data correcting codes:** methods for storing data in such a way that small changes can be easily detected and automatically corrected.
- **Digital signatures**

Tools for availability

- **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges.

- **Computational redundancies:** computers and storage devices that serve as fallbacks in the case of failures.

Tools for assurance

- **Trust management**
  - **Policies,** which specify behavioral expectations that people or systems have for themselves and others.
    - For example, the designers of an online music system may specify policies that describe how users can access and copy songs.
  - **Permissions,** which describe the behaviors that are allowed by the agents that interact with a person or system.
    - For instance, an online music store may provide permissions for limited access and copying to people who have purchased certain songs.
  - **Protections,** which describe mechanisms put in place to enforce permissions and polices.
    - We could imagine that an online music store would build in protections to prevent people from unauthorized access and copying of its songs.

Tools for authenticity

- **Digital signatures.** These are cryptographic computations that allow a person or system to commit to the authenticity of their documents in a unique way that achieves **nonrepudiation**, which is the property that authentic statements issued by some person or system cannot be denied.

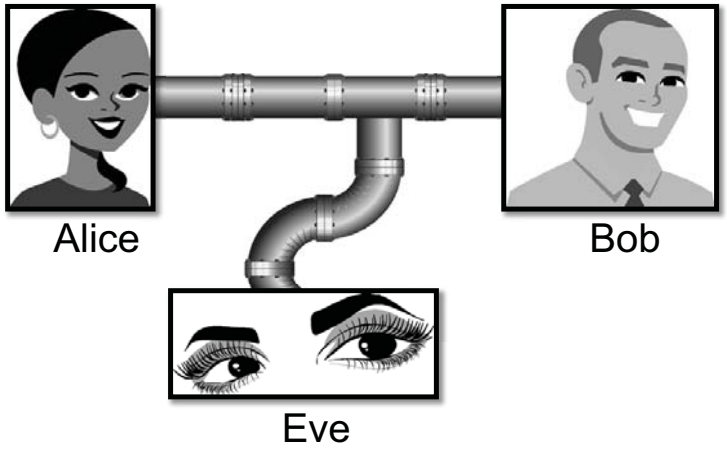
Tools for anonymity

- **Aggregation:** the combining of data from many individuals so that disclosed sums or averages cannot be tied to any individual.
- **Mixing:** the intertwining of transactions, information, or communications in a way that cannot be traced to any individual.
- **Proxies:** trusted agents that are willing to engage in actions for an individual in a way that cannot be traced back to that person.
- **Pseudonyms:** fictional identities that can fill in for real identities in communications and transactions, but are otherwise known only to a trusted entity.

Threats and Attacks

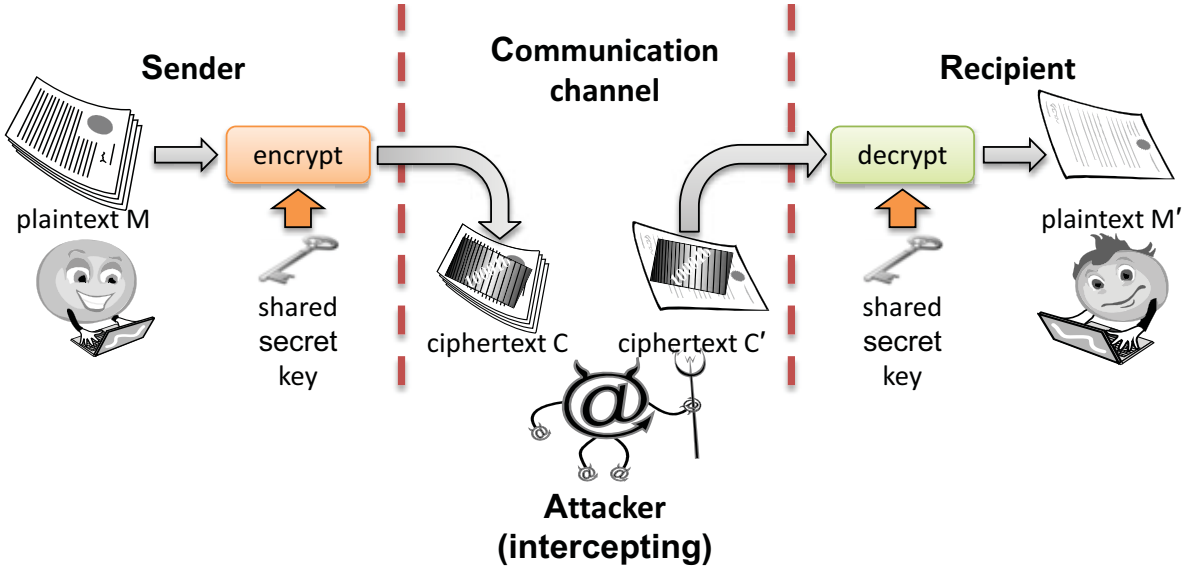
- Threat to confidentiality
  - Eavesdropping
- To integrity
  - Alteration/tampering
- To availability
  - Denial-of-service
- To authenticity
  - Masquerading
- To assurance
  - Repudiation
- To anonymity
  - Correlation and traceback
- Social engineering

Eavesdropping



- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel.

Alteration



- **Alteration:** unauthorized modification of information.
  - **Example:** the **man-in-the-middle attack,** where a network stream is intercepted, modified, and retransmitted.

Denial of Service

- **Denial-of-service**: the interruption or degradation of a data service or information access.
  - Example: request flooding attacks to take down a web server

Masquerading

"From: Alice"
(really is from Eve)

- **Masquerading:** the fabrication of information that is purported to be from someone who is not actually the author.

Repudiation

- **Repudiation:** the denial of a commitment or data receipt.
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.

Correlation and traceback

- **Correlation** and **traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.

Social Engineering

- **Social engineering:** refers to the psychological manipulation of people into performing actions or divulging confidential information
  - **Pretexting**: creating a story that convinces an administrator or operator into revealing secret information.
  - **Phishing:** fraudulently obtaining private information
  - **Baiting:** offering a kind of "gift" to get a user or agent to perform an insecure action.
  - **Quid pro quo (something for something):** offering an action or service and then expecting something in return.
    - "survey": giving out passwords for a cheap pen

The Ten (classic) Security Principles

Economy of mechanism

- This principle stresses **simplicity** in the **design** and **implementation** of security measures.
  - While applicable to most engineering endeavors, the notion of simplicity is especially important in the security domain, since a simple security framework facilitates its understanding by developers and users and enables the efficient development and verification of enforcement methods for it.

Fail-safe defaults

- This principle states that the default configuration of a system should have a **conservative protection scheme**.
  - For example, when adding a new user to an operating system, the default group of the user should have minimal access rights to files and services. Unfortunately, operating systems and applications often have default options that favor usability over security.
  - This has been historically the case for a number of popular applications, such as web browsers that allow the execution of code downloaded from the web server.

Complete mediation

- The idea behind this principle is that every access to a resource must be checked for **compliance with a protection scheme**.
  - As a consequence, one should be wary of performance improvement techniques that save the results of previous authorization checks, since permissions can change over time.
  - For example, an online banking web site should require users to sign on again after a certain amount of time, say, 15 minutes, has elapsed.

Open design

- According to this principle, the security architecture and **design** of a system should be made **publicly available**.
  - Security should rely only on keeping cryptographic keys secret.
  - Open design allows for a system to be scrutinized by multiple parties, which leads to the early discovery and correction of security vulnerabilities caused by design errors.
  - The open design principle is the opposite of the approach known as **security by obscurity,** which tries to achieve security by keeping cryptographic algorithms secret and which has been historically used without success by several organizations.

Separation of privilege

- This principle dictates that **multiple conditions** should be required to achieve access to restricted resources or have a program perform some action.

Least privilege

- Each program and user of a computer system should operate with the bare **minimum privileges necessary** to function properly.
  - If this principle is enforced, abuse of privileges is restricted, and the damage caused by the compromise of a particular application or user account is minimized.
  - The military concept of **need-to-know** information is an example of this principle.

Least common mechanism

- In systems with multiple users, mechanisms allowing resources to be **shared by more than one user should be minimized**.
  - For example, if a file or application needs to be accessed by more than one user, then these users should have separate channels by which to access these resources, to prevent unforeseen consequences that could cause security problems.

Psychological acceptability

- This principle states that user interfaces should be **well designed and intuitive**, and all security-related settings should adhere to what an ordinary user might expect.

Work factor

- According to this principle, the **cost of circumventing** a security mechanism should be compared with the resources of an attacker when designing a security scheme.
  - A system developed to protect student grades in a university database, which may be attacked by snoopers or students trying to change their grades, probably needs less sophisticated security measures than a system built to protect military secrets, which may be attacked by government intelligence organizations.

Compromise recording

- This principle states that sometimes it is more desirable to **record the details** of an intrusion than to adopt more sophisticated measures to prevent it.
  - Internet-connected surveillance cameras are a typical example of an effective compromise record system that can be deployed to protect a building in lieu of reinforcing doors and windows.
  - The servers in an office network may maintain logs for all accesses to files, all emails sent and received, and all web browsing sessions.

Tool: access control

- Which users can read/write which files?
- Are my files really safe?
- What does it mean to be root?
- What do we really want to control?

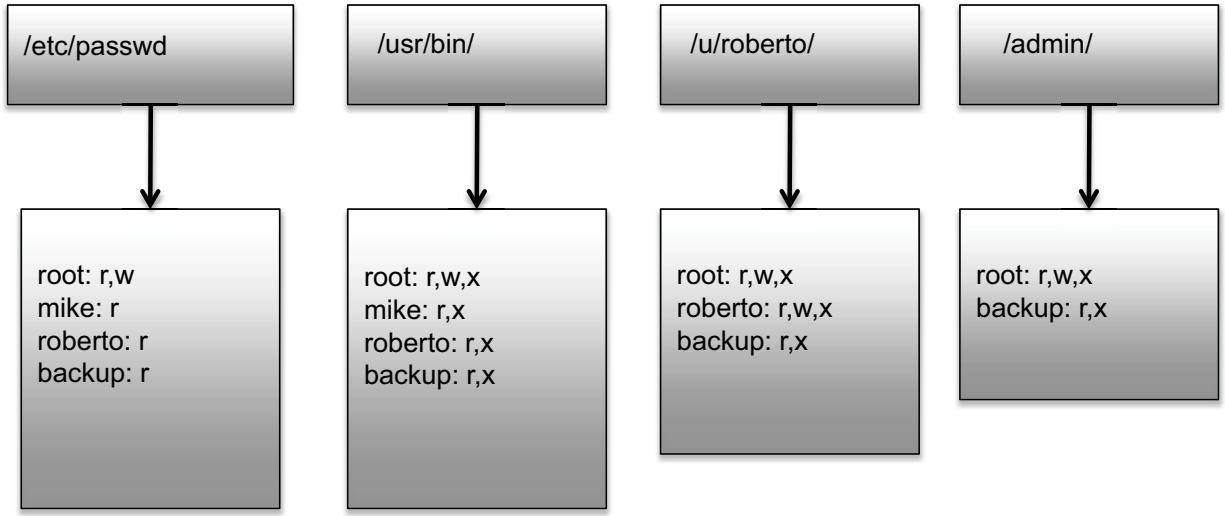
Access control matrices

- **A table that defines permissions**.
  - Each row of this table is associated with a **subject,** which is a user, group, or system that can perform actions.
  - Each column of the table is associated with an **object,** which is a file, directory, document, device, resource, or any other entity for which we want to define access rights.
  - Each cell of the table is then filled with the access rights for the associated combination of subject and object.
  - Access rights can include actions such as reading, writing, copying, executing, deleting, and annotating.
  - An empty cell means that no access rights are granted.

Example

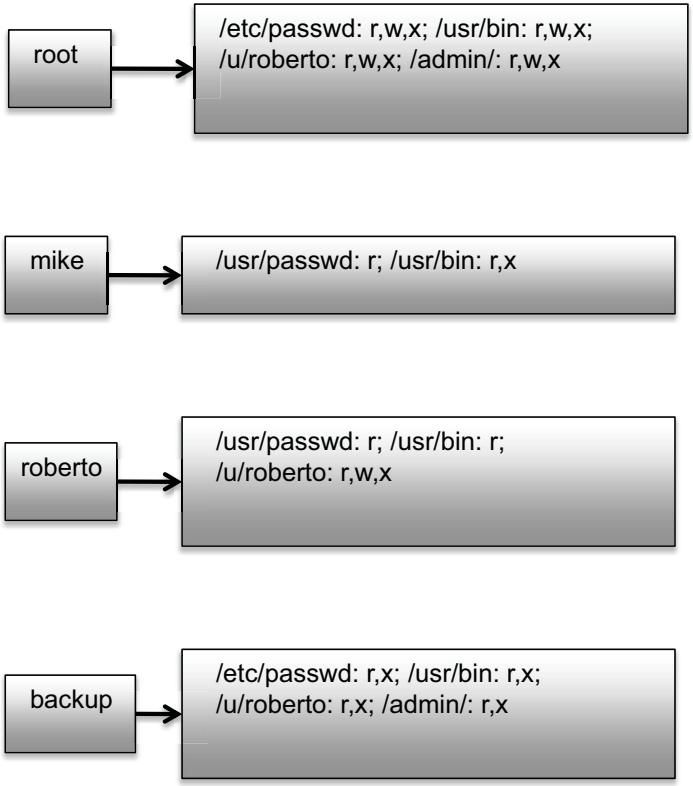
	/etc/passwd	/usr/bin/	/u/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec
mike	read	read, exec		
roberto	read	read, exec	read, write, exec	
backup	read	read, exec	read, exec	read, exec
...	...	...	...	...

Access control lists



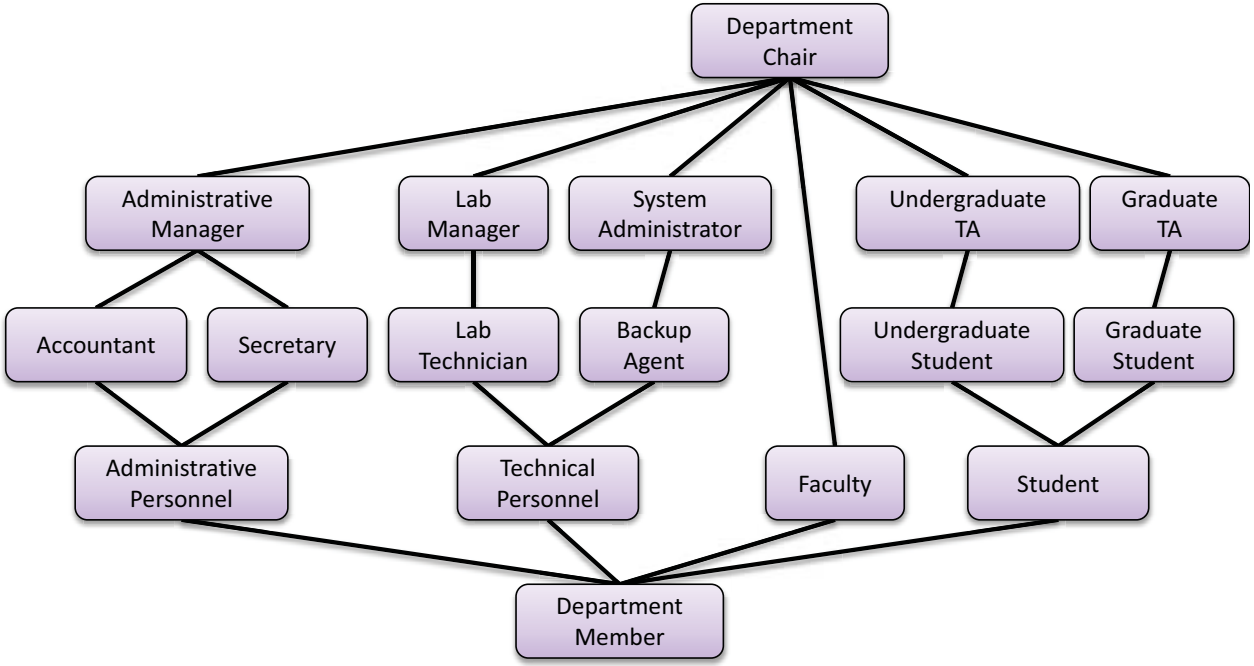
- It defines, for each object, o, a list, L, called o's access control list, which enumerates all the subjects that have access rights for o and, for each such subject, s, gives the access rights that s has for object o.

Capabilities



- Takes a subject- centered approach to access control. It defines, for each subject s, the list of the objects for which s has nonempty access control rights, together with the specific rights for each such object.

Role-based access control



- Define **roles** and then specify access control rights for these roles, rather than for subjects directly.

Looking forward

- Wrapping up tools
- Accountability
- OS security