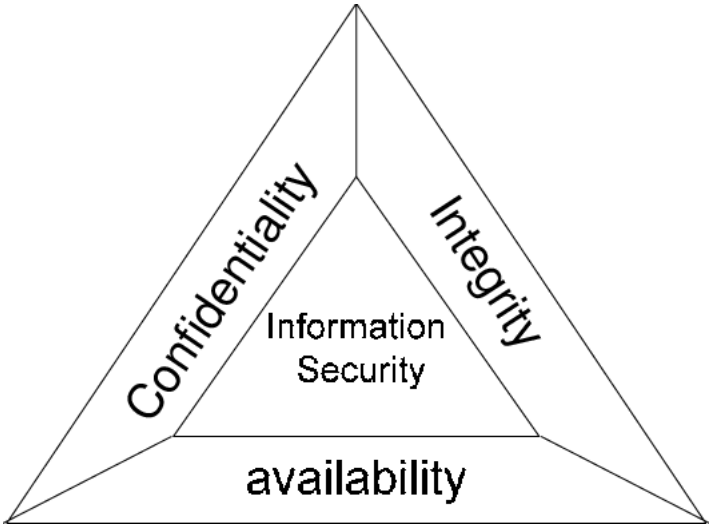
MAJOR GOALS OF SECURITY

Goals of security can be defined using the C-I-A Triad shown in the figure below.



C-I-A stands for: Confidentiality, Integrity and Availability.

- **Confidentiality:**

This is the prevention of unauthorized disclosure of information. The confidentiality service provides for the secrecy of information. When properly used, confidentiality only allows authorized users to have access to information. In order to perform this service properly, the confidentiality service must work with the accountability service to correctly identify individuals. In performing this function, the confidentiality service protects against the access attack. The confidentiality service must take into account the fact that information may reside in physical form in paper files, in electronic form in electronic files, and in transit. It involves keeping information secret or private and ensures that information is accessed only by authorized personnel.

- **Integrity:**

The integrity service provides for the correctness of information. When properly used, integrity allows users to have confidence that the information is correct and has not been modified by an unauthorized individual. As with confidentiality, this

service must work with the accountability service to properly identify individuals. The integrity service protects against modification attacks. Information to be protected by the integrity service may exist in physical paper form, in electronic form, or in transit. Integrity means that there is an external consistency in the system - everything is as it is expected to be. It ensures that information is modified only by authorized personnel

- **Availability:**

The availability service provides for information to be useful. Availability allows users to access computer systems, the information on the systems, and the applications that perform operations on the information. Availability also provides for the communications systems to transmit information between locations or computer systems. The information and capabilities in terms of availability are all electronic. It is the prevention of unauthorized withholding of information. Information should be accessible and useable upon appropriate demand by an authorized user. It ensures that information and systems can be accessed when needed by authorized personnel

The work of the information security (IS) specialist is to provide highly available and reliable data to authorized persons only when they need it. The C-I-A triad is a way to remember that the confidentiality, integrity, and availability of information is the concern of every IS specialist.

Minor goals of security

- **Non-repudiation:**

This is the prevention of either the sender or the receiver denying a transmitted message. A system must be able to prove that certain messages were sent and received. Non-repudiation is often implemented by using digital signatures.

- **Authentication:**

This is proving that you are who you say you are, where you say you are, at the time you say it is. Authentication can be accomplished by using any combination of three things:

– Something you know (like a password or PIN)

– Something you have (like a smart card or a badge)

– Something you are (like fingerprints or a retina scan)

- **Access Control:**

This can be described as the limitation and control of access through identification and authentication. A system needs to be able to identify and authenticate users for access to data, applications and hardware.

In a large system there may be a complex structure determining which users and applications have access to which objects.

- **Accountability:**

The system managers are accountable to scrutiny from outside. Audit trails must be selectively kept and protected so that actions affecting security can be traced back to the responsible party. The primary reason is that the accountability service does not protect against attacks by itself. It must be used in conjunction with other services to make them more effective. Accountability by itself is the worst part of security; it adds complications without adding value. Accountability adds cost and it reduces the usability of a system. However, without the accountability service, both integrity and confidentiality mechanisms would fail.