Examples of Security Requirements

Some examples of applications that illustrate the security requirements are provided.

- ✓ Confidentiality - Student grade information is an asset whose confidentiality is considered to be highly important by students. Grade information should only be available to students, their parents, and employees that require the information to do their job. Student enrollment information may have a moderate confidentiality rating. This information is seen by more people on a daily basis, is less likely to be targeted than grade information, and results in less damage if disclosed. Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a school's Web site.
- ✓ Integrity – Consider a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital. The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible. Patient allergy information is an example of an asset with a high requirement for integrity. Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.
- ✓ Availability - The more critical a component or service, the higher is the level of availability required. Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks. The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss.

1. **Confidentiality**: This means keeping secrets safe. When something is confidential, it's meant to be kept private and only shared with authorized people. If confidentiality is breached, it means someone has shared secret information without permission.

2. **Integrity**: Integrity is about making sure information stays accurate and complete. Imagine if someone changed your homework answers or deleted important parts of your essay without you knowing—that would be a breach of integrity. It's important to ensure that information can't be tampered with or destroyed in the wrong way.

3. **Availability**: Availability is ensuring that you can get to information when you need it. Imagine if you couldn't access your favorite website or your phone suddenly stopped working—that would be a loss of availability. It's important for information and systems to be reliable and accessible when they're supposed to be.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

• Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

• Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.