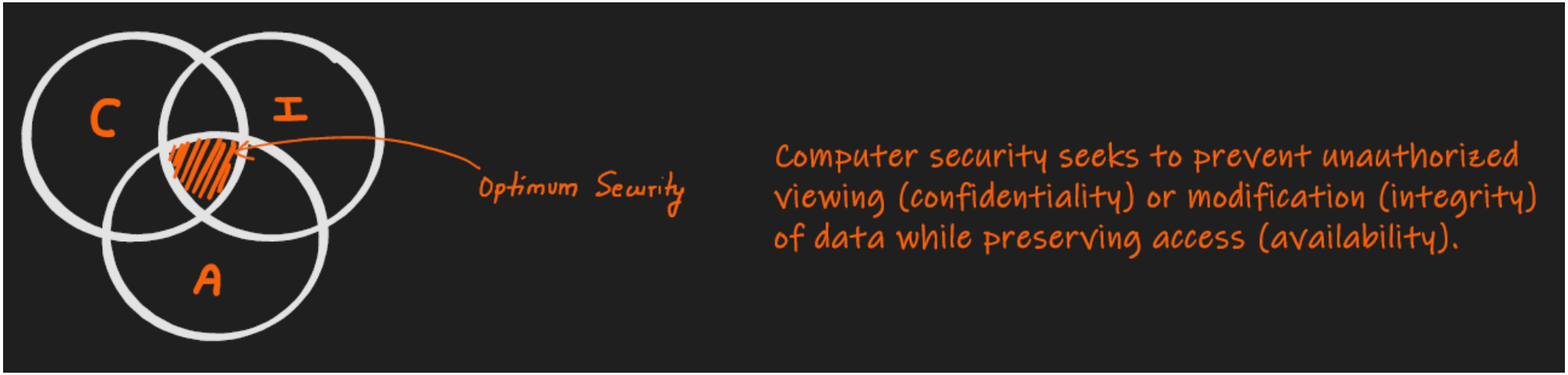
Module 1: Introduction and Number Theory

Goals of Security



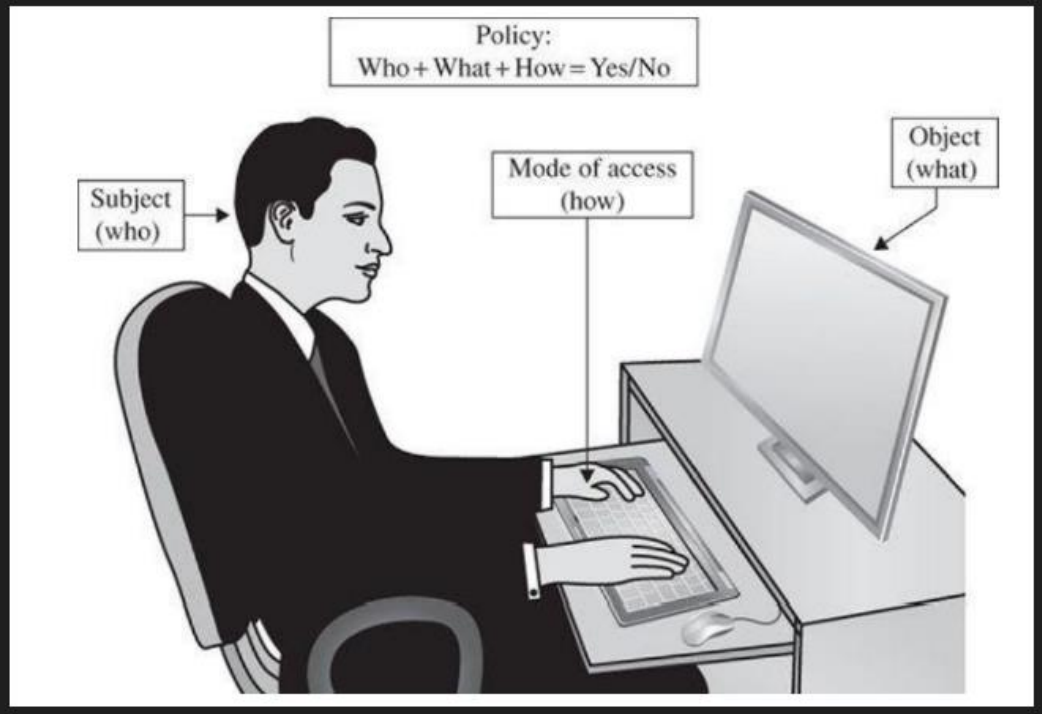
Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Threats to Confidentiality

Interception, Sniffing

Steps to ensure Confidentiality



A person, process, or program is (or is not) authorized to access a data item in a particular way. We call the person, process, or program a subject, the data item an object, the kind of access (such as read, write, or execute) an access mode, and the authorization a policy

Integrity –

Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Threats to Integrity

Fabrication , Modification

Examples of integrity failures are easy to find. A number of years ago a malicious macro in a Word document inserted the word "not" after some random instances of the word "is;" you can imagine the havoc that ensued.

Steps to ensure Integrity

Integrity can be enforced in much the same way as can confidentiality: by rigorous control of who or what can access which resourcesm in what ways

Availability

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Threats to Availability

Interruption

A computer user's worst nightmare: You turn on the switch and the computer does nothing. Your data and programs are presumably still there, but you cannot get at them. Fortunately, few of us experience that failure

Steps to ensure Availability

- There is a timely response to our request.
- Resources are allocated fairly so that some requesters are not favored over others.
- Concurrency is controlled; that is, simultaneous access, deadlock management, and exclusive access are supported as required.
- The service or system involved follows a philosophy of fault tolerance, whereby hardware or software faults lead to graceful cessation of service or to work-arounds rather than to crashes and abrupt loss of information.
- The service or system can be used easily and in the way it was intended to be used.