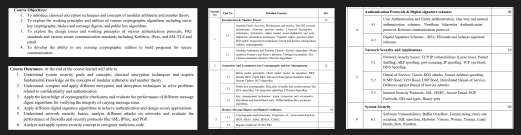
Lecture No. 1

Cryptography & System Security

Topic: Introduction








Text Books:

1. William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
2. Behrouz A. Forouzan, —Cryptography & Network Security‖, Tata Mc Graw Hill
3. Bernard Menezes, —Cryptography & Network Security‖, Cengage Learning.
4. Network Security Bible, Eric Cole, Second Edition, Wiley.

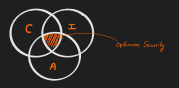
Reference Books:

1. Applied Cryptography, Protocols Algorithms and Source Code in C, Bruce Schneier, Wiley.
2. Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.

Topic (Goals): By 9.10, 19.37

## Security Goals

## Confidentiality, Integrity & Availability




Optimum Security

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability).

### 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 caused.

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 resources 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.

Topic (Concept): By 28

## Vulnerability, Threat & Control

### Vulnerability

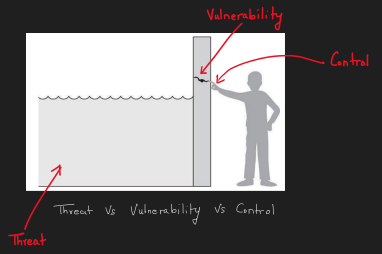
A vulnerability is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

### Threat

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

### Control

Controls prevent threats from exercising vulnerabilities.




Threat Vs Vulnerability Vs Control

Here, a wall is holding water back. The water to the left of the
wall is a threat to the man on the right of the wall:

The water could rise, overflowing onto the man, or it could stay beneath the height of the wall, causing the wall to collapse.

So the threat of harm is the potential for the man to get wet, get hurt, or be drowned. For now, the wall is intact, so the threat to the man is unrealized

However, we can see a small crack in the wall—a vulnerability that threatens the man's security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man.