

Security Basics

Main goals of Security:

- Confidentiality
- Integrity
- Availability

Confidentiality: This could be explained by the following examples,

- An attacker cannot read password or credit card details over the network.
- Thief cannot read off a stolen laptop.
- An intruder cannot find out about the process time, CPU usage and memory usage.
- One should be able to hide facts that they made any communication over the network at all.
- Maintain anonymity/privacy.

Integrity: This could mean the following,

- Only authorized users can modify file or databases.
- Integrity can be used to detect violation of DB constraints.
- Grant program execution or file access permissions.
- An attacker cannot modify a message while it is in transit.
- Users should be able to accept only unmodified messages.

Availability: By availability we mean that,

- An attacker cannot deny user access to any site (DoS).
- Attacker cannot use a users CPU time/ all disk space.
- Attacker cannot prevent access to printers, RAM etc.

Security vs Reliability:

Faults can always occur in worst possible combinations. So we need a “Threat Model”, which defines the capabilities and limitations of an attacker.

Limitations of an attacker:

- Limited Computation.
- Bandwidth: on today’s Internet, hackers can have a very large bandwidth.
- Limited time and money
- Expertise: The skills of a hacker may vary.
Eg: Script kiddie, corporate espionage
- Knowledge: hacker may know the hardware configuration, OS version, Application version, Configuration information of the target machine.
- They may not know passwords, Random Number Generators (RNG) output.

Local vs Remote:

In a local attack, the attacker has an account on the system while in a remote attack, the attack is over a network.

Active vs Passive:

A passive attacker only listens to information over the network while an active attacker may send/modify/suppress messages. It is usually harder to catch a passive listener.