SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

UNIT I INTRODUCTION

Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple Levels, Security Policies - Model of Network Security - Security Attacks, Services and Mechanisms - OSI security architecture - classical encryption techniques: substitutiontechniques, transposition techniques, steganography - Foundations of modern cryptography: perfect security - information theory - product cryptosystem - cryptanaysis

1.1 SECURITY TRENDS

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)

This definition introduces three key objectives that are at the heart of computer security:

- **Confidentiality:** This term covers two related concepts:
- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may bedisclosed.
- **Integrity:** This term covers two related concepts:
- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability:** Assures that systems work promptly and service is not denied to authorized users

These three concepts form what is often referred to as the **CIA triad** (Figure 1.1). The three concepts embody the fundamental security objectives for both data and for information and computing services

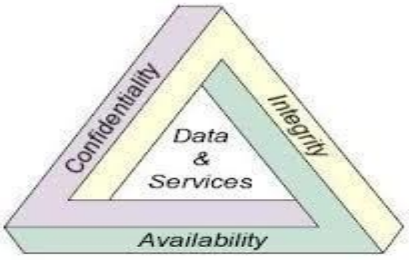


Figure 1.1 CIA triad

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 as follows:

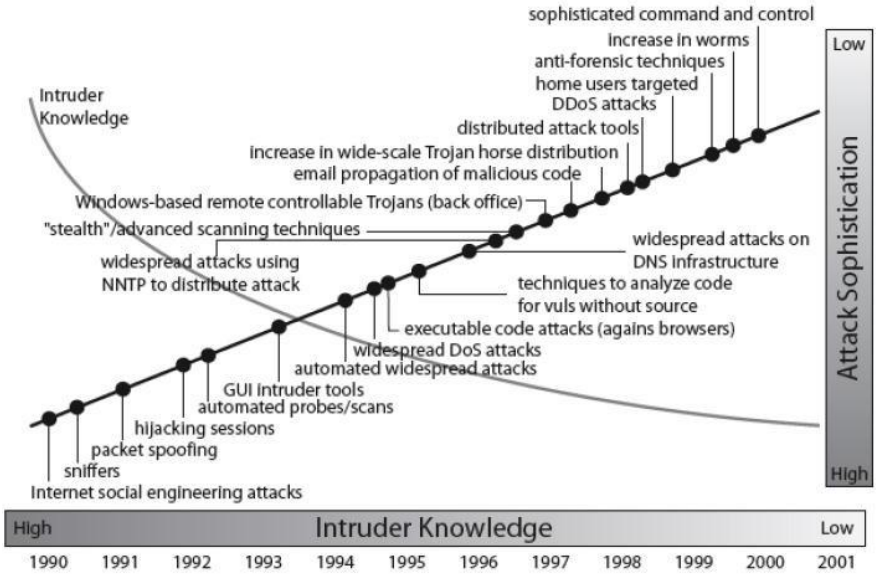
• **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

• **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

• **Computer Security -** Generic name for the collection of tools designed to protect data and to thwart hackers**.**

• **Network Security -** Measures to protect data during their transmission.

• **Internet Security -** Measures to protect data during their transmission over a collection of interconnected networks Our Focus is on Internet Security which consists of measures to deter, prevent, detect and correct security violations that involve the transmission and storage of information



Source: CERT

Figure 1.2 Security Trends

1.1.1 THE CHALLENGES OF COMPUTER SECURITY

Computer and network security is both fascinating and complex. Some of the reasons follow:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given selfexplanatory, one-word labels: confidentiality, authentication, non repudiation, or integrity

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.

3. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement and in a logical sense

.

5. Security mechanisms typically involve more than a particular algorithm or protocol

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantagethat the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. There is a natural tendency on the part of users and system managers to perceive littlebenefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today‟s short-term,overloaded environment.

9. Security is still too often an afterthought to be incorporated into a system after the design iscomplete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment toefficient and user-friendly operation of an information system or use of information.