A MODEL FOR NETWORK SECURITY

B Tech CSE- IV Sem

TCS 491

Introduction to Cryptography

Jan- Jun 2022

- **A sample model**

- A message is to be transferred from one party to another across some sort of Internet service.
- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.
- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who m may present a threat to confidentiality, authenticity, and so on.
- All the techniques for providing security have two components:

■ A security-related transformation on the information to be sent..

■ Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

NOTE: A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

- The general model shows that there are four basic tasks in designing a particular security service:
- 1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- 2. Generate the secret information to be used with the algorithm.
- 3. Develop methods for the distribution and sharing of the secret information.
- 4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

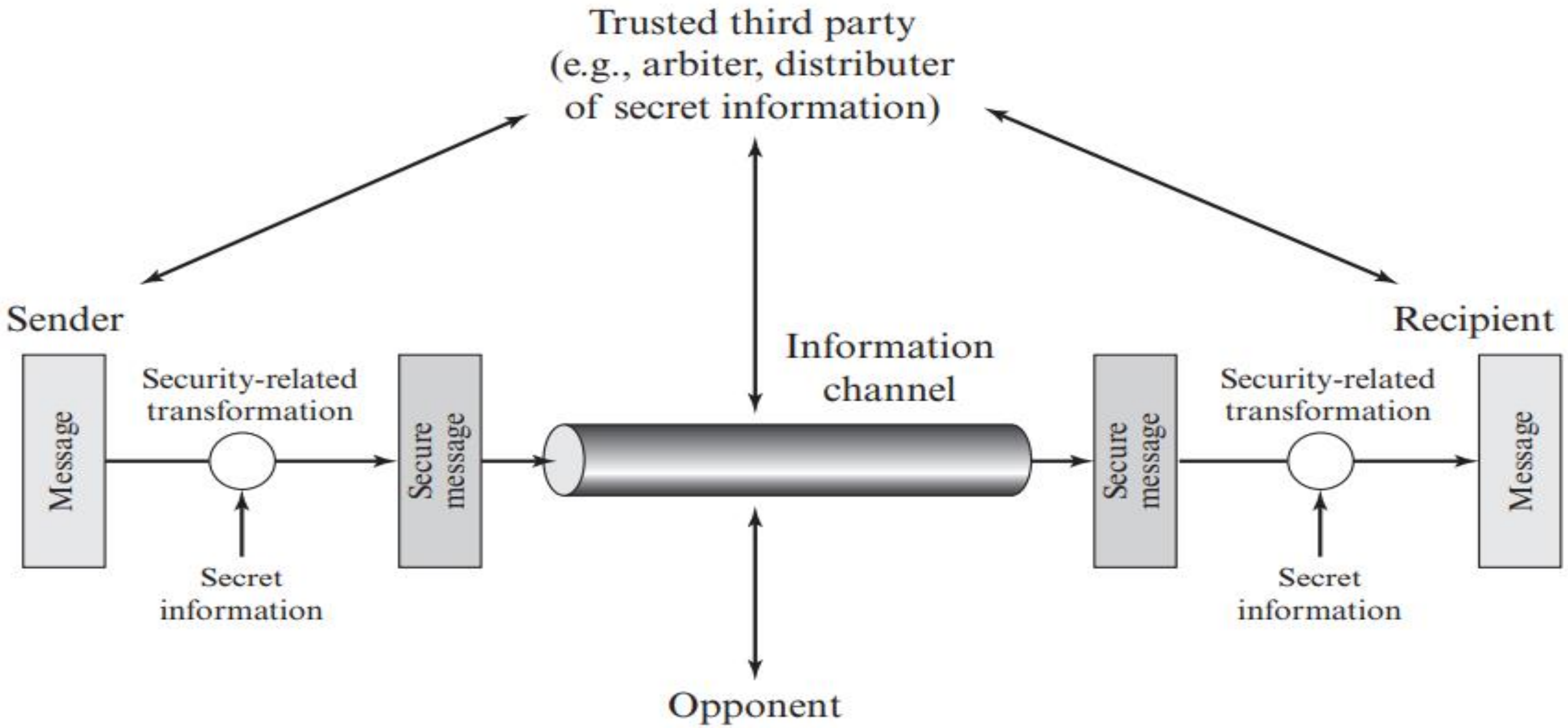

Figure 1.5 Model for Network Security

Network Access Security Model

- Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

■ Information access threats: Intercept or modify data on behalf of users who should not have access to that data.

■ Service threats: Exploit service flaws in computers to inhibit use by legitimate users

Attackers: Two Types

- 1. Human attacker(Hacker)
- 2. Software Attacker:
- Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

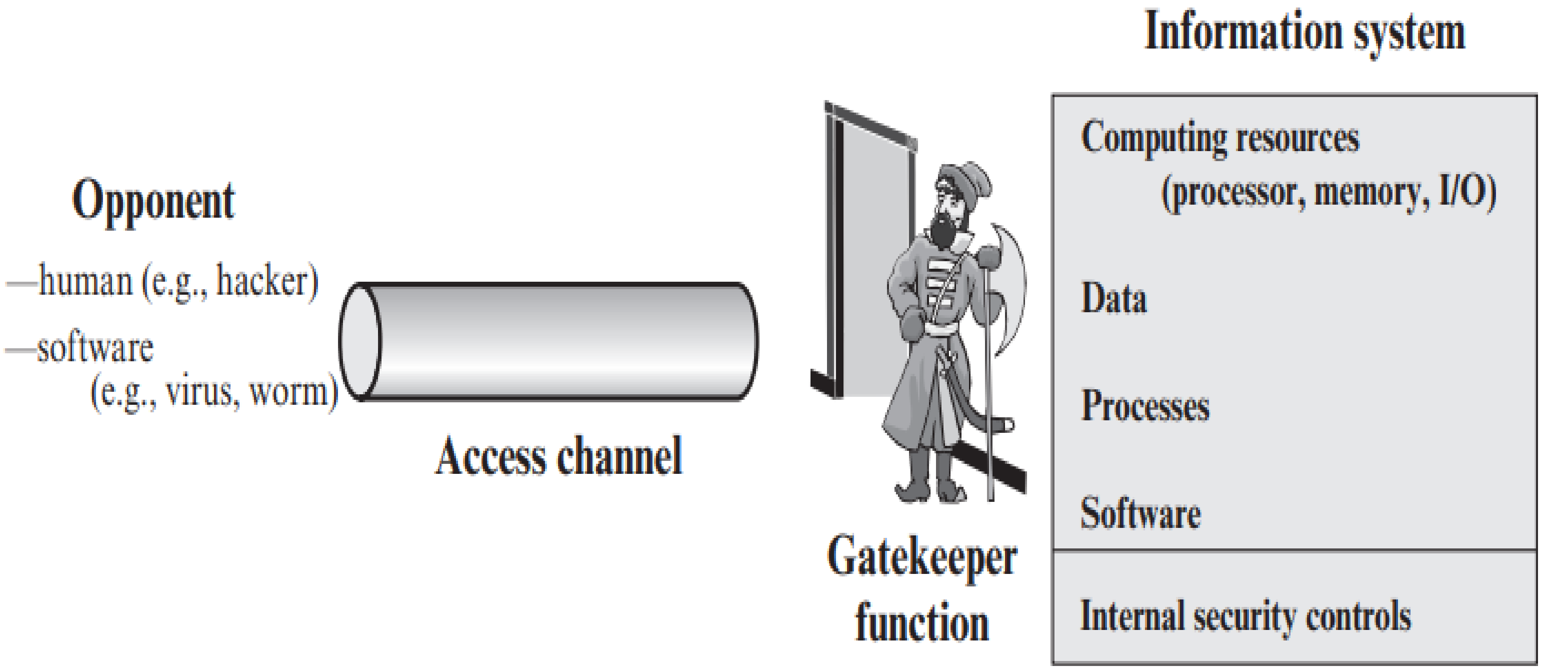

Figure 1.6 Network Access Security Model

- The security mechanisms needed to cope with unwanted access fall into two broad categories.
- **Gatekeeper Function:**
- The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- **Internal Controls:**
- Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

STANDARDS

- Many of the security techniques and applications described in this book have been specified as standards. Additionally, standards have been developed to cover management practices and the overall architecture of security mechanisms and services.
- Throughout this b s book, we describe the most important standards in use or that are being developed for various aspects of cryptography and network security. Various organizations have been involved in the development or promotion of these standards.
- The most important (in the current context) of these organizations are as follows:
- **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY:** NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.
- **INTERNET SOCIETY:** ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).
- **ITU-T:** The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the development of technical standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations.
- **ISO**: The International Organization for Standardization (ISO)7 is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.

Thank You

&

Best Wishes