Chapter 8. Secure Communication Protocols: Authentication, Authorization and Key Distribution

In this chapter, we study applied cryptographic protocols, used to secure communication and distributed systems. Specifically, we discuss protocols for entity authentication, key distribution, and authorization (also called access control). Most of our discussion is generic, but we also give some details of the Kerberos authentication and key distribution system.

8.1. Communication Networks and Internetworking

We begin with a brief review of data communication networks, focusing on the terminology and architecture of the Internet (often referred to as TCP/IP, after the two key protocols). Readers interested in more details are encouraged to consult one of the numerous textbooks covering this area, e.g. [P92, S00], while readers who are familiar with this subject may skip through this section and proceed to the next one.

The Internet is a huge, global network, which is composed of many individual, different computer communication *networks.* Each network provides communication services between at least two computers. Different networks may have different ownership, management and policies, as well as different technologies, protocols and topologies. Typical networks are illustrated in Figure 8.1, and include:

- A point-to-point connection between only two computers, often called a *link.*
- A *local area network (LAN),* often using broadcast technologies over shared cable (e.g. Ethernet) or over the air (wireless LAN). Typical topologies for wired LAN are a *star* network, where all computers connect thru a central *hub;* a *bus* network, where all computers connect via shared bus or cable; and a *ring* network, where computers are connected to each other, forming a ring.

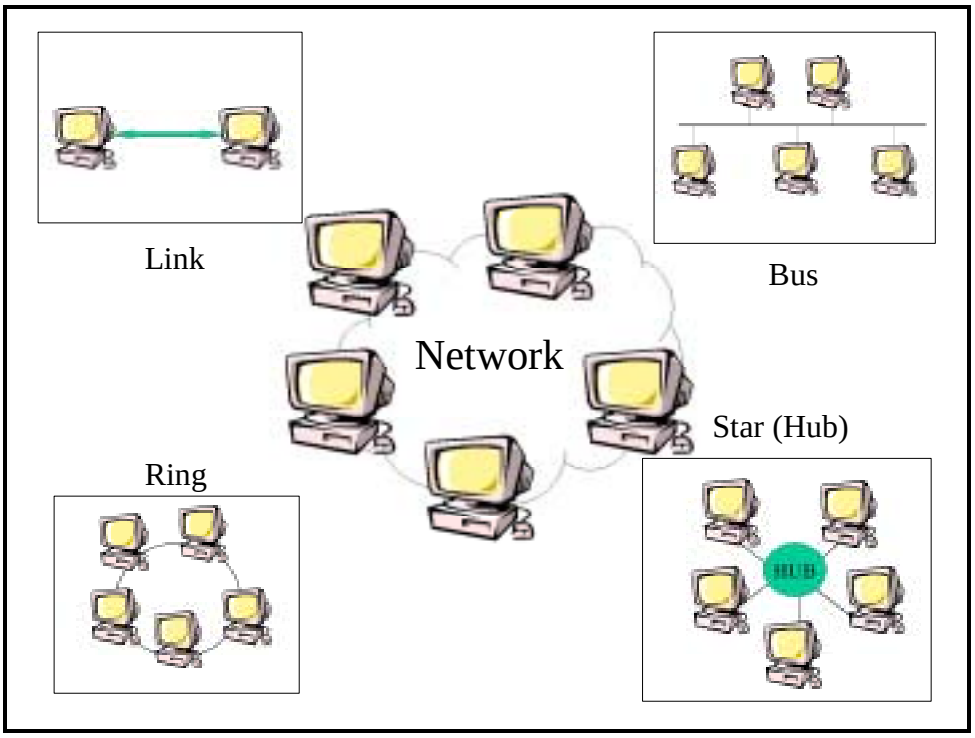
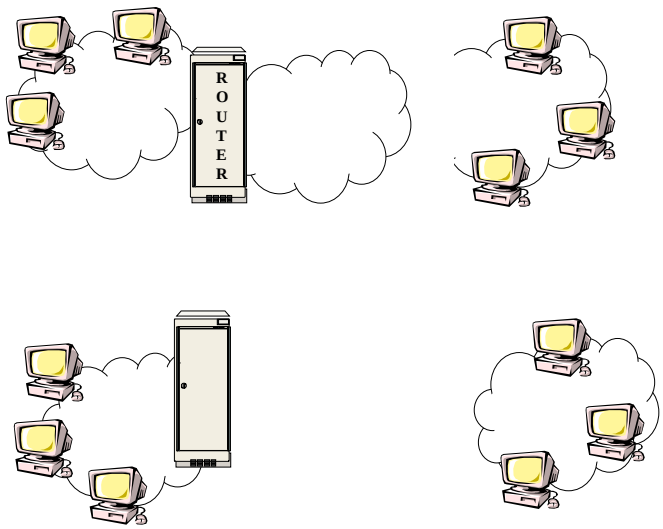


Figure 8.1: Typical Computer Communication Networks

An *internet* is a collection of two or more networks, allowing communication between the computers in all the networks. The use of capital first letter distinguishes the specific, global Internet from the general concept of an internet. The Internet society defines standards for internet protocols; this family of protocols is usually referred to as TCP/IP, after the two most important protocols in it – TCP (Transmission Control Protocol) and IP (Internet Protocol). We focus on TCP/IP internets and internetworking protocols.

Communication in internets is facilitated by special computers called *routers* (or gateways), which are members of two or more networks. We illustrate an internet in Figure 8.2, where networks are denoted by clouds, except for links between routers which are denoted by a direct line. Messages (often called *packets)* whose destination is not in the current network are sent to a router connected to the network, which then forwards it on one of the networks it is connected to, either directly to the destination (if on one of the networks connected to the router) or to another router (hopefully closer to the destination). This function is called *routing*, and to know the correct route (where to send a packet) we use a *routing protocol.*


ROUTER