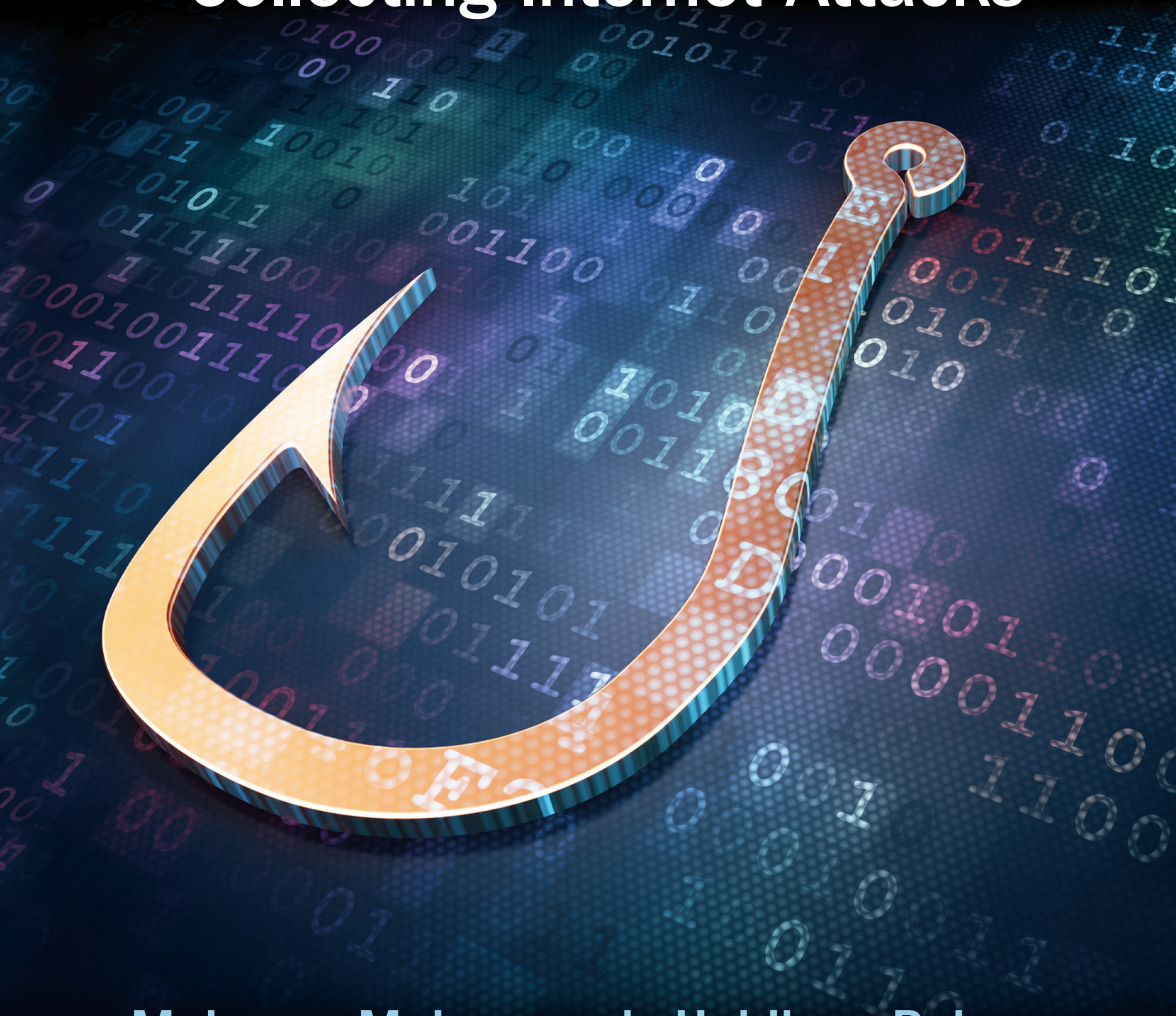
Honeypots and Routers

Collecting Internet Attacks



Mohssen Mohammed · Habib-ur Rehman

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Honeypots and Routers

Collecting Internet Attacks

Honeypots and Routers

Collecting Internet Attacks

Mohssen Mohammed · Habib-ur Rehman

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20151028

International Standard Book Number-13: 978-1-4987-0220-1 (eBook - PDF)

Contents

1

Computer Networks

HABIB-UR REHMAN

A computer network typically comprises three components: devices, medium, and topology. Computers, smartphones, laptops, routers, switches, and repeaters are the different kinds of devices that may exist in a computer network. In order to communicate with each other, these devices are connected by a medium, either wireless or wired. The resulting schematic of the devices linked through the medium is the topology of the network.

In a computer network, communication actually happens among devices. In the context of human conversations, the term *communication* encompasses a complete dialog between two persons. The same rule applies to computer networks: communication among two or more devices may consist of more than one message exchanged among the participating devices. *Session* is a more widely used technical term to describe a series of correlated messages exchanged among devices.

Before we move further into our discussion of computer networks, let us recall the example of postal service commonly described in the textbooks to explain how a computer network functions. A house may have more than one resident, who can be a sender or receiver of messages. All these residents share the same address; however, the actual sender/recipient is identified by the name mentioned on the envelope. The postal service is usually neither the sender nor the recipient but the messages pass through it, and it facilitates the transmission of messages. The recipient address is used to deliver the message to its destination and the source address is used to identify its originator. The message itself is usually some data or information arranged in a comprehensible way for the recipient. The overall assembly of the message should also be comprehensible for the postal service, so that the sender and recipient addresses are distinguishable, identifiable, and locatable.

When computers communicate, constraints such as being comprehensible, distinguishable, or identifiable require precise and comprehensive establishment of the procedures and regulations for the delivery of message(s). This brings the fourth component of computer networks into the picture: the protocol. Protocols and standards are the set of rules and procedures followed by the devices during communication.

This chapter is divided into four sections, each reviewing one of the four components of the computer network.

1.1 Devices

A device typically plays one of the three roles in a message exchange: it originates a message, or it is the recipient of the message, or the message passes through it. The device initiating a message is usually called *source* or *origin*, while the recipient(s) of a message is (are) called *destination(s)* or *sink(s)*. Together the two are called *end nodes* or *end devices*. When the two end devices are not connected directly, the message passes through one or more intermediate devices. The end devices are generally the computing devices used by the end users such as PCs, phones, and tablets (tabs); on the other hand, the intermediate devices are usually special-purpose devices with the objective of facilitating the transmission between the end devices.

Based on its role in the communication, a device has to perform several steps in a particular order to make the communication successful. For example, the job of the source device is to specify the address of only the destination device and not that of the destination or intermediate devices. The open systems interconnection (OSI) reference model, as it is usually called, is a conceptual description of the tasks and duties performed by devices while communicating in a computer network. This abstract model divides the activities, based on their relevance and dependency, into seven groups referred to as *layers*: physical, data link, network, transport, session, presentation, and application (Figure 1.1).

The primary purpose of a computer communication is to facilitate the users and deliver the data or information. The user interacts with the computer system, the device of our communication scenario, through some application; the data or information provided to the system or received from the system is usually in a user comprehensible format. Due to this fact, the end devices generally perform all the

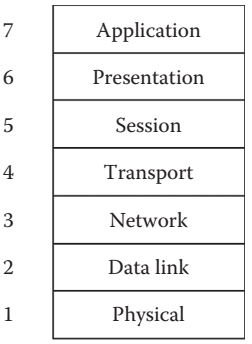


Figure 1.1 ISO/OSI reference model for network communication.

actions described in the OSI model, or in other words, implement all the seven layers. The intermediate nodes, on the other hand, might be implementing a limited number of layers (or performing tasks related to fewer layers) according to their role in the communication. One way to categorize the devices in a computer network is to group them according to the layer they belong.*

As mentioned earlier, the user mostly interacts with the end devices, which are typical computing devices. However, the communication always involves multiple intermediate devices sitting in the core of the network joining the two ends. Next, we mention the four important categories of intermediate devices commonly participating in a computer communication.

1.1.1 Modem

The job of a modem is to convert digital signals to analog signals and vice versa. Modems are generally required when devices perform digital communication over the telephone network. By definition, a modem performs *mo*dulation and *dem*odulation only, a task that belongs to OSI layer 1. However, in almost all the cases, the functionality of the appropriate layer 2 is part of the device.

* The presence of the functionality of an upper OSI layer in a device requires that it should perform the tasks of all the lower layers as well, that is, it should implement all the layers up to that level. Hence, if we say a device is a layer 3 device or belongs to layer 3, this means that it implements (or performs the actions associated with) all the layers from layer 1 to layer 3.

1.1.2 Bridge

A bridge is a device that operates at layer 2 of the OSI reference model and connects two smaller networks together into one, so that the devices in the two segments can communicate with each other. The devices are connected to the bridge through its ports individually in most of the cases. However, multiple bridges can also be joined through the same ports when more than two smaller networks are combined. Bridges are commonly referred to as *switches*, although, the term *switch* has broader technical meanings. Further details of the functionality of the bridges are mentioned in Section 1.4.1.

1.1.3 Router

Routers are also devices that combine one or more networks into one; however, they belong to layer 3 of the OSI model. This implies that routers perform more and complicated tasks as compared to bridges. Typically, unlike bridges, the devices are not directly connected to the ports of the router; it is in fact the bridges that are connected to the routers. Multiple routers can also be connected to each other to combine the networks attached to each of them. The operations and characteristics of the routers are also described later in Section 1.4.2.

1.1.4 Gateway

Imagine a student in China who wants to send his admission request to a university in Canada by postal service. What happens if he writes the recipient address only in the Chinese language; how would the postal staff in Canada deliver it? When two networks following different communication protocols or standards are joined together, a network device is required to perform the job of translation or, in technical terms, *conversion*; such a device is called *gateway*. The functionality of the protocol conversion or translation can be required at different levels or layers; hence, gateways can belong to different layers. For example, we can say that a modem works as a physical layer gateway device. The common practice while designing a computer network is to follow the same protocol in the entire network attached to a single router. Hence, the need of a gateway usually arises when

two routers (following different protocols/standards) are connected together. In such a situation, the functionality of the gateway is implemented as an additional software component inside the router, resulting in a router working as a gateway too.

It is important to mention here that in most of the present-day computer networking scenarios, the devices that we see around us sometimes perform more than one of the above-mentioned roles. A very common example is the home routing device, which has the functionality of a bridge as well as a router. Similarly, the typical DSL modems available these days combine the functionality of a modem, bridge, gateway, as well as router.

1.2 Medium

The computer network medium is of two major types: wire and wireless. As the name suggests, in the wired medium the message propagates in a physical *wire* used to connect the devices. In a wireless medium, on the other hand, the message propagates in free space in the form of radio or infrared waves.

1.2.1 Wired Networks

Copper wire is the most common form of medium used in the wired computer networks. Coaxial and twisted pair cables are the two widely used copper wire or cable types. In dial-up Internet access, plain old telephone service lines are used to connect a computer to the Internet. The plain old telephone service lines are also copper wires and a computer requires a modem to communicate over this kind of wire. The fourth common type is the fiber optic cable, a thin cable or fiber of glass or plastic that works as a *pipe of light*.

Twisted pair. As the name suggests, a twisted pair cable is made of thin copper wires twisted together. Multiple pairs of wires, shielded or unshielded, are bundled together in a cable. Twisted pair cable is the most widely used cable type for computer networks and telephone networks due to its lower cost and easy handling. It has several types and categories, based on quality, construction, purpose, and data rate supported. The highest-grade twisted pair cables can achieve data rates up to 1 Gbps;

however, most of the variations can carry signals up to 100 m without significant strength loss.

Coaxial. The coaxial cable has a copper wire in the center with a layer of insulation around it. Around this insulation layer, there is another layer of copper in the form of a gauze and a final outer insulation jacket. It was a common type of computer networking cable before the introduction of twisted pair cables. Still, it is commonly used for cable TV and cable Internet.

Fiber optic. In fiber optic cable, the signal is transmitted in the form of a light beam or wave inside the glass or plastic fiber. Multiple fibers are bundled together usually in a cable. A single fiber can carry multiple light waves, and it is possible to achieve very high data rates from each wave as compared to the copper wires. Furthermore, the effect of interference and attenuation is very low, which makes it possible to transmit the signal over longer distances. Due to its very high data rates and higher cost, fiber optic cable is not used to interconnect individual computers; rather it is used to combine networks.

1.2.2 Wireless Networks

Wireless networks are of two major categories: in the first, radio waves carry the data; in the second infrared waves carry the data. The radio-based wireless networks are more common since the infrared waves can only travel in a straight line and cannot penetrate through walls. One important characteristic of the wireless medium is that it is always shared because the signal travels in open space, which is accessible to all.

1.3 Network Topology

Network topology could be either physical or logical. A physical topology describes how the devices are physically linked with each other and what kind of medium is used for those links. The logical topology, on the other hand, is an abstract view of the physical

topology with unnecessary details hidden. Thus, a physical topology can have multiple logical topologies produced after filtering the irrelevant details. The relationship between the two terms can be better described with the example of a layout or plan for a building. A detailed plan of a building will have all the details such as walls, doors, electric wiring, water lines, and sewer lines, just the way a physical topology has all the details of the computer network. However, we can also have a layout of electric wiring only for a building; such a plan is analogous to the logical topology in computer networks. Devices in a computer can be interconnected using different approaches; hence, it is possible to have different kinds of physical topologies.

The area physically covered by a computer network is another important aspect with respect to the topology. Primarily, it is due to the varying technical limitations of different media types. A classical approach to classify the networks is based on the geographical area covered by them. Local area network (LAN), metropolitan area network (MAN), and wide area network (WAN) are the three main categories. In the beginning, LANs, MANs, and WANs were distinguished based on the area covered; the administrative boundaries of a network and the relevance in the purpose of the devices participating in the network are some of the additional factors that contribute to decide the category to which a network belongs.

1.3.1 Wide Area Network

A WAN is a network that comprises devices distributed over a vast area, for example, a state or a continent, or even bigger. Thus, the Internet is usually referred to as a WAN; in fact, it is the largest WAN. Similarly, the nationwide network of some Internet service provider is also an example of WAN.

1.3.2 Local Area Network

A LAN is usually limited to a building or a group of adjacent buildings under one administration. The geographical limits of LAN are not that precise and terms such as *campus area network* are also used

in situations when the area covered by a LAN is significantly large. However, technically, a network is considered a LAN when all the participating devices are interconnected using privately laid physical topology and is under one administration. This definition also leads us to the conclusion that when an organization's business is spread over a metropolitan area or wide area, in almost all the cases the organization's MAN or WAN is *logically* spread over the physical network laid by some other organization, usually the owner of the public telephone and data networks in that area.

The protocols and technologies used in LANs and WANs are also different, once again mainly due to the different attenuation features of the physical medium used.

1.4 Network Protocols and Standards

Although devices and medium are the physical components of a computer network, the importance of protocols is no less in the success of communication, as devices require a well-established plan to follow. Protocols describe actions to be performed and guidelines to be followed by the devices during communication. As mentioned earlier, the OSI reference model is the fundamental document of communication in computer networks. Protocols in most of the cases target the work plan of the OSI model; however, there is no single protocol that targets all the seven layers of the OSI model. A single protocol usually targets the job of an individual layer and protocols are always associated with the respective OSI layer. In order to perform communication, a device follows multiple protocols, which work in a cooperative fashion. This necessitates that protocols should be compliant to each other. Due to this fact, protocols evolve in the form of families or groups, where a family constitutes of protocols belonging to different OSI layers and compliant to each other.

The category of protocols and standards is in fact very rich and endless; however, in this section, we will limit our discussion to the relevant items from this list. The term *standard* in computer networks loosely refers to a protocol or model or an architecture or a combination thereof that is designed or ratified by some established authority or organization, such as IEEE, for wider commercial use.

ASSEMBLY OF A MESSAGE

An important principle to consider while reviewing the protocols is how a message is assembled before its actual transmission over the medium. In our communication model, it is in fact the user who wants to send a message using his or her device. This message is captured by some application on the device and will now go through a series of the protocols. Every protocol before passing on this message to the next protocol in the chain arranges the content of the message in a particular order usually referred to as *protocol data unit* (PDU) or sometimes simply a *packet*. Hence, PDU is a collection of bits or bytes or characters pertaining to the user message and some additional information for the convenience of the next protocol. This additional administrative information is usually placed in the beginning of the PDU and hence called the *header* of the PDU. In most of the cases, the next protocol in the chain only looks into the header for the necessary information and do not parse rest of the PDU.

1.4.1 IEEE 802 Standards Family

The IEEE 802 is a group of standards for LANs and MANs. It targets the communication tasks belonging to the first two layers of the OSI model. The IEEE 802 LAN and MAN reference model further divides the data link layer into two sub layers: medium access control (MAC) and logical link control, as shown in Figure 1.2 [1].

The IEEE 802 LANs and MANs are packet-based networks where message is transmitted as a sequence of data octets; most of the commercially available devices and applications are supported by these standards. The packets are technically referred to as *frames* at this level. The MAC sublayer is primarily responsible for the connectionless frame transfer between the two devices, while logical link control is more concerned with the services such as management, security, or acknowledgment (Figure 1.3) [1].

The IEEE 802 standards family has individual standards for several types of physical medium, as displayed in Figure 1.4. Each standard is

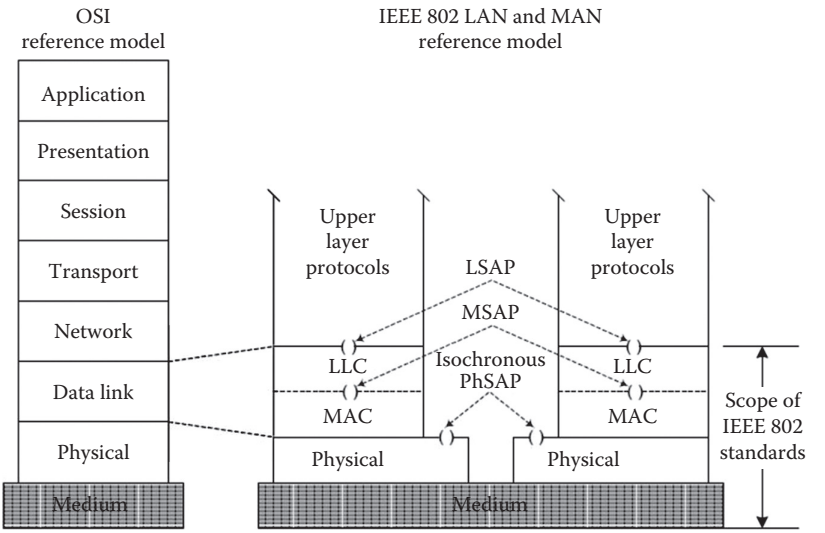


Figure 1.2 IEEE 802 LAN and MAN reference model for end stations. LLC—logical link control, MAC—medium access control, LSAP—link service access point, MSAP—MAC service access point, and PhSAP—physical service access point. (Data from *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, IEEE Std 802®-2001 [R2007].)

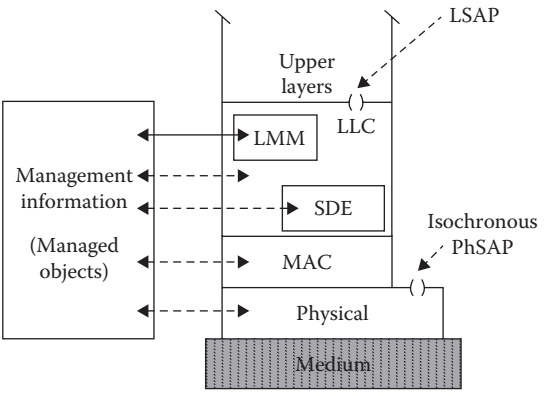


Figure 1.3 IEEE 802 reference model with end-station management and security. LMM—LAN/MAN management and SDE—secure data exchange. (Data from *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, IEEE Std 802®-2001 [R2007].)

a collection of protocols and guidelines for a certain physical medium and the relevant MAC layer, for example, Ethernet, wireless LAN, and broadband wireless MANs. All kinds of MAC provide a common service with core features to the logical link control through the MAC service access point [1].