## Key term

### Chapter 1

Computer security – A broad term that has many meanings and related terms, but in a general sense entails the methods used to ensure that a system is secure.

Critical infrastructure – Critical infrastructures are those whose loss or impairment would have severe repercussions on society.

Elite hackers – Elite hackers are the best of the best, and are characterized by the skill level necessary to discover and exploit new vulnerabilities.

Hacker – with individuals who conduct this activity (hacking) being referred to as hackers

Hacking – The term used by the media to refer to the process of gaining unauthorized access to computer systems and networks.

### Chapter 2

*-property(star poverty) – The second security principle enforced by the Bell-LaPadula security model.

Access control – This refers to all security features used to prevent unauthorized access to a computer system or network.

Auditability – The condition that a control can be verified as functioning.

Authentication – This ensures that an individual is who they claim to be before allowing them to access information they are authorized to access.

Availability – This ensures that the data, or the system itself, is available for use when the authorized user wants it.

Bell-LaPadula security model – A security model first utilized by the U.S. military (data confidentiality is a chief concern for the military and is essential to its operations).

## Chapter 4

Backdoor – Avenues that can be used to access a system while circumventing normal security mechanisms.

Dumpster diving – The process of going through a target's trash, searching for information that can be used in an attack, or gaining knowledge about a system or network.

Phishing – A scam wherein an e-mail user is duped into revealing personal or confidential information that the scammer can use illicitly.

Piggybacking – This is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.

Reverse social engineering – This technique is similar to social engineering in that attackers are attempting to obtain information that can be used in an attack.

Social engineering – The art of deceiving another individual so that they reveal confidential information. This is often accomplished by posing as an individual who should be entitled to have access to the information.

(noted the difference between Reverse social engineering and Social engineering)

## Chapter 5

Algorithm – A step-by-step procedure; typically an established computation for solving a problem within a set number of steps.

Block cipher – A cipher that operates on blocks of data.

Ciphertext – the encrypted output.

Plaintext – the unencrypted input text.

Collision attack – An attack on a hash function, in which a specific input is generated to produce a hash function output that matches another input.

Confusion - is a principle to affect the randomness of an output.

Hash(-ing) function – a special mathematical function performs a one-way fuction, which means that once the algorithm is processed, there is no feasible way to use the ciphertext to retrieve the plaintext that was used to generate it.

Encrypt - The secret writing that enables an individual to hide the contents of a message or file from all but the intended recipient.

## Chapter 8

Access tokens – This is defined as "something you have."

Autoplay – when CD/DVD or USB containing an inserted application, the computer promotes for input versus requiring the user to explore the device filesystem and find the executable file.

Biometrics – This is used to verify an individual's identity to the system or network using something unique about the individual, such as a fingerprint, for the verification process. Examples include fingerprints, retinal scans, hand and facial geometry, and voice analysis.

BIOS passwords – Password protection that allows you to boot the machine but requires a password to edit any BIOS settings.

Bootdisk – Any media used to boot a computer into an operating system that is not the native OS on its hard drive could be classified as a bootdisk.

UPS – an uninterruptible power supply is used to protect against short-duration power failures.

Cable shielding – can be employed to avoid interference.

Backup power – are used to protect against a long-duration power failure.

## Chapter 9

Address Resolution Protocol (ARP) – This protocol in the TCP/IP suite specification is used to map an IP address to a Media Access Control (MAC) address.

Bus topology – This network layout has a common line (the bus) that connects devices.

Datagram – This is a packet of data that can be transmitted over a packet-switched system in a connectionless mode.

Denial-of-service (DoS)– This is an attack in which actions are taken to deprive authorized individuals from accessing a system, its resources, the data it stores or processes, or the network that it's connected to.

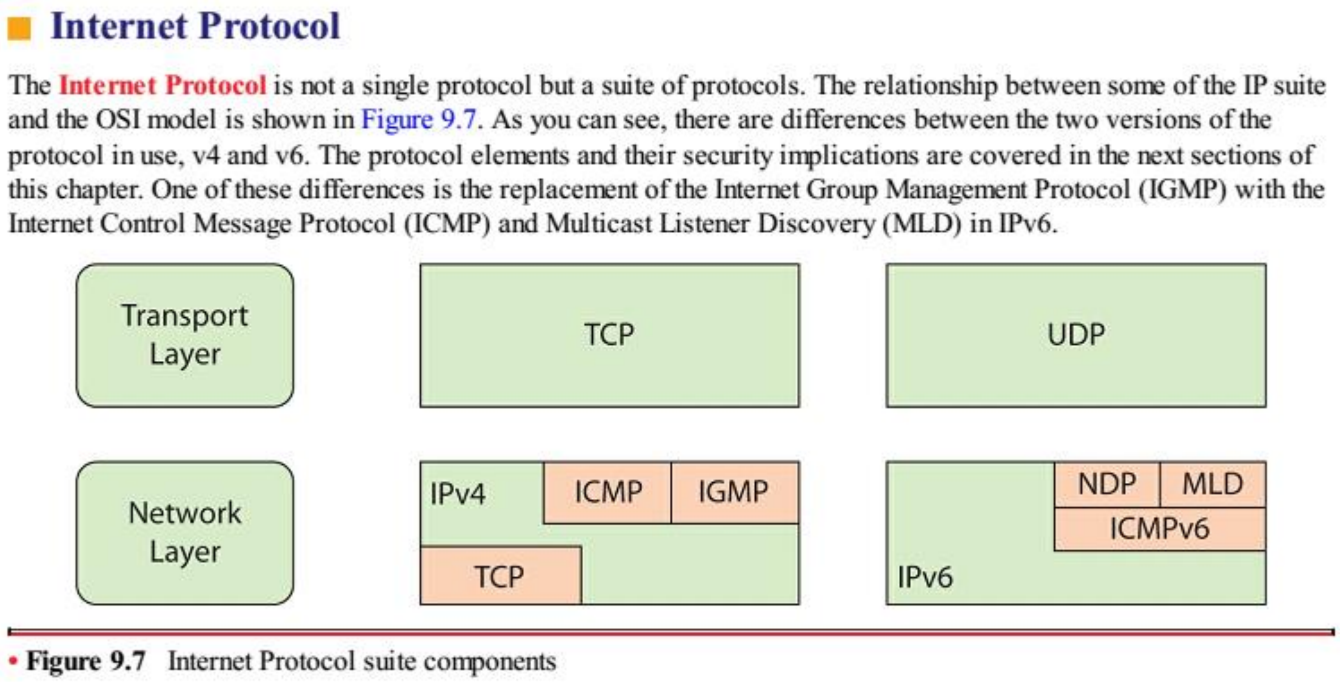
Domain Name System (DNS) – This service \translates an Internet domain name (such as www.mcgrawhill.com) into IP addresses.

Topology – one major component of every network's architecture show how the network is physically or logically arranged.

Star topology – network components are connected to a central point.

Bus topology – network components are connected to the same cable.(the bus / the backbone)

Ring topology – network components are connected to each other in a close loop with each device directly connected to two other devices.



## Internet Protocol

The **Internet Protocol** is not a single protocol but a suite of protocols. The relationship between some of the IP suite and the OSI model is shown in Figure 9.7. As you can see, there are differences between the two versions of the protocol in use, v4 and v6. The protocol elements and their security implications are covered in the next sections of this chapter. One of these differences is the replacement of the Internet Group Management Protocol (IGMP) with the Internet Control Message Protocol (ICMP) and Multicast Listener Discovery (MLD) in IPv6.

• **Figure 9.7** Internet Protocol suite components

Security zones – different zones are designed to provide layers defense, with the outermost layers providing basic protection and the innermost layers providing the highest level of protection.

Intranet – a connection of networks which is used to transport information. Lies inside the trusted area of a network and is under the security control of the system and network administrators.

Extranet – is an extension of a selected portion of a company's intranet to extranet partners.

VLAN tunneling (virtual local arear network) – a logical network allowing system on different physical networks to interact as if the were connected to the same physical network.

## Chapter 11

Authentication, authorization, and accounting (AAA) – These are three common functions performed upon system login. Authentication and authorization almost always occur, with accounting being somewhat less common.

Access control – These mechanisms or methods are used to determine what access permissions subjects (such as user) have for specific objects (such as files).

Access control list(ACL) – is a set of rules used to control traffic flow into or out of an interface or network.

Accounting – This is a collection of billing and other detail records.

Administrator (account) – are reserved for special functions and typically have much more access and control over the computer than the average user account.

User – applies to any person accessing a computer system.

Permission – what the user is allowed to do with objects on system—which files he may access, which program he may execute.

Group – under privilege management, a group is a collection of users with common criteria.

Password policy – has the following components: password construction, reuse restriction, duration, protection of passwords, consequences.

Single sign on(SSO) – is a form of authentication that involves the transferring of credentials between systems.

Rule-based access control (RBAC) – This is an access control mechanism based on rules.

Remote access process – the process of connecting by remote access involves two elements: a temporary network connection and a series of protocols to negotiate privileges and commands.

Authentication – This is the process by which a subject's (such as a user's) identity is verified.

Kerberos – This is a network authentication protocol designed by MIT for use in client/server environments.

FTP – File Transfer Protocol is a plaintext protocol that operates by communicating over TCP between a client and a server.

VPN – a virtual private network is a secure virtual network build on top of a physical network.

## Chapter 13

Analysis engine – The analysis engine examines the collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database. The analysis engine is the "brains" of the IDS.

Anomaly detection model – This model relies heavily on a predefined set of attack and traffic patterns called signatures.

Banner grabbing – is a technique used to gather information from a service that publicizes information via a banner.

Content-based signature – This is a signature based on the data within a packet.

Context-based signature – This is a signature based on information such as source, destination, and other network activity data.

Honeypots – also called digital sandbox, is an artificial environment where attackers can be contained and observed without putting real systems at risk.

IDS (intrusion detection system) – is a security system that detects inappropriate or malicious activity on a computer or network.

HIDS (host-based IDS) – examines activity on an individual system, such as a mail server, web server, or individual PC. It is concerned only with an individual system and usually has no visibility into the activity on the network or system around it.

NIDS (network-based IDS) – examines activity on the network itself. It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.

## Chapter 15

Auditing – is done to verify the accuracy and integrity of financial records in the financial community.

Backdoor – This is a hidden method used to gain access to a computer system, network, or application. Often used by software developers to ensure unrestricted access to the systems they create. Synonymous with trapdoor.

Birthday attack – This is a form of attack in which the attack needs to match not a specific item but just one of a set of items.

Botnet – This is a collection of software robots, or bots, that runs autonomously and automatically and commonly invisibly in the background. The term is most often associated with malicious software, but it can also refer to the network of computers using distributed computing software.

Buffer overflow – This is a specific type of software coding error that enables user input to overflow the allocated storage area and corrupt a running program.

Hacker – with individuals who conduct this activity (hacking) being referred to as hackers

Hacking – The term used by the media to refer to the process of gaining unauthorized access to computer systems and networks.

Denial-of-service (DoS) attack – This is an attack in which actions are taken to deprive authorized individuals from accessing a system, its resources, the data it stores or processes, or the network to which it is connected.

Distributed denial-of-service (DDoS) attack – A special type of DoS attack in which the attacker elicits the generally unwilling support of other systems to launch a many-against-one attack.

Social engineering – The art of deceiving another individual so that they reveal confidential information. This is often accomplished by posing as an individual who should be entitled to have access to the information.

Phishing – This is the use of social engineering to trick a user into responding to something such as an e-mail to instantiate a malware-based attack.

Malware – or malicious code, refer to software that has been designed for some nefarious purpose.

TCP/IP hijacking – used to refer to the process of taking control of an already existing session between a client and a server.

Remote access trojans (RATs) – are malware designed to enable remote access to a machine. It is hidden in the system which enable attackers to have a way back into system.