UNIT -5

Routing security

- Routing security has received varying levels of attention over the past several years and has recently begun to attract more attention specifically around Border Gateway Protocol (BGP) on the public Internet. Despite this new attention, however, the area most open to attack is often not the Internet's BGP tables but the routing systems within your own enterprise network. Because of some of the sniffing-based attacks, an enterprise routing infrastructure can easily be attacked with man-in-the-middle and other attacks designed to corrupt or change the routing tables with the following results:
- **Traffic redirection**—In this attack, the adversary is able to redirect traffic, enabling the attacker to modify traffic in transit or simply sniff packets.
- **Traffic sent to a routing black hole**—Here the attacker is able to send specific routes to null0, effectively kicking IP addresses off of the network.
- **Router denial-of-service (DoS)**—Attacking the routing process can result in a crash of the router or a severe degradation of service.
- **Routing protocol DoS**—Similar to the attack previously described against a whole router, a routing protocol attack could be launched to stop the routing process from functioning properly.
- **Unauthorized route prefix origination**—This attack aims to introduce a new prefix into the route table that shouldn't be there. The attacker might do this to get a covert attack network to be routable throughout the victim network.

Link layer connectivity

- the link layer is responsible for transporting information from one host (or router) to another over a *single* link
- each network-layer datagram is encapsulated in a link-layer *frame*
- two fundamentally different types of link-layer channels:
    - *broadcast* channels
        - common in local area networks (LANs), wireless LANs, etc.
        - many hosts connected to the same communications channel
        - *medium access protocol* is needed to coordinate transmissions
    - *point-to-point* communications link
        - used between two routers or home dial-up modem and ISP router
        - coordination is trivial

    - still issues around framing, reliable transfer etc.

- All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be divided into the following categories:
- **Interruption**
- Interruption is a security threat in which availability of resources is attacked. For example, a user is unable to access its web-server or the web-server is hijacked.
- **Privacy-Breach**
- In this threat, the privacy of a user is compromised. Someone, who is not the authorized person is accessing or intercepting data sent or received by the original authenticated user.
- **Integrity**
- This type of threat includes any alteration or modification in the original context of communication. The attacker intercepts and receives the data sent by the sender and the attacker then either modifies or generates false data and sends to the receiver. The receiver receives the data assuming that it is being sent by the original Sender.

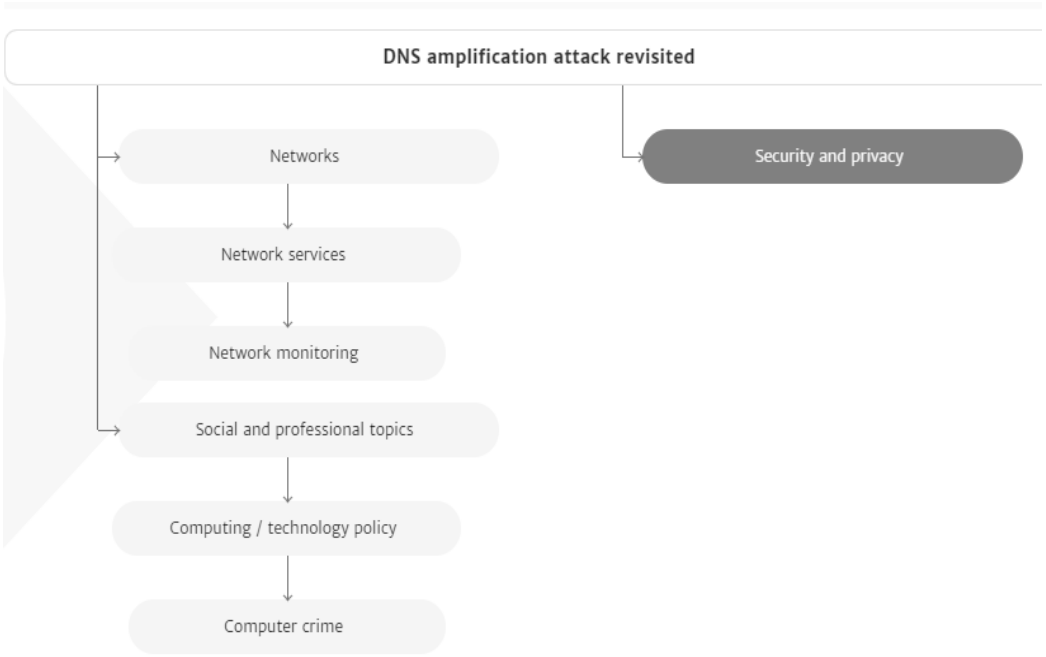
TCP/IP Model

- The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:
- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer
- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

DNS REVISITED

- It is without doubt that the Domain Name System (DNS) is one of the most decisive elements of the Internet infrastructure; even a slight disruption to the normal operation of a DNS server could cause serious impairment to network services and thus hinder access to network resources. Hence, it is straightforward that DNS nameservers are constantly under the threat of Denial of Service (DoS) attacks. This paper presents a new, stealthy from the attacker's viewpoint, flavor of DNSSEC-powered amplification attack that takes advantage of the vast number of DNS forwarders out there. Specifically, for augmenting the amplification factor, the attacker utilizes only those forwarders that support DNSSEC-related resource records and advertize a large DNS size packet. The main benefits of the presented attack scenario as compared to that of the typical amplification attack are:
- (a) The revocation of the need of the aggressor to control a botnet, and (b) the elimination of virtually all traces that may be used toward disclosing the attacker's actions, true identity and geographical location. The conducted experiments taking into consideration three countries, namely Greece, Ireland and Portugal demonstrate that with a proper but simple planning and a reasonable amount of resources, a determined perpetrator is able to create a large torrent of bulky DNS packets towards its target. In the context of the present study this is translated to a maximum amplification factor of 44.



WEAKNESS OF INTERNET SECURITY

- Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.
- In today's digital landscape, many of our daily activities rely on the internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online. This means that tons of data and sensitive information are constantly being shared over the internet. The internet is mostly private and secure, but it can also be an insecure channel for exchanging information. With a high risk of intrusion by hackers and cybercriminals, internet security is a top priority for individuals and businesses alike.

1.Malicious software:

- An internet user can be tricked or forced into downloading software that is of malicious intent onto a computer. Such software comes in many forms, such as viruses, Trojan horses, spyware, and worms.
- Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to

some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

- A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.
- Computer Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.

2.Denial-of-service attacks:

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Another way of understanding DDoS is seeing it as attacks in cloud computing environment that are growing due to the essential characteristics of cloud computing. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. According to businesses who participated in an international business security survey, 25% of respondents experienced a DoS attack in 2007 and 16.8% experienced one in 2010.DoS attacks often use bots (or a botnet) to carry out the attack.

3.Phishing:

- Phishing is an attack which targets online users for extraction of their sensitive information such as username, password and credit card information.Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex subdomains hide the real website host. Insurance group RSA said that phishing accounted for worldwide losses of $10.8 billion in 2016.