Cryptography and Network Security

Km Simran Jaiswal(20CS60R58)

20-Sep-2020

1 Introduction

For understanding network security we need to know that"How computer network works"?.Whenever we load a URL we are trying to communicate to web server,based on certain protocols a virtual connection is established between user's computer to web server. There are many challenges during network communication such as I.P. addressing and routing.

2 URL(Uniform Resource Locator)

Unique identifier used to locate a resource on the internet. Format of URL is: $< scheme >: // < user >:< password > @ < host >:< port > / < URL - path >? < query - string >$

3 Network Layer Model

Network layer model consist of 5 layers:

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer
5. Physical Layer

Users can only see application layer.Applications like web browsers and email clients rely on the application layer to initiate communications.
Each layer are dependent only on the functionality provided by layer below it.

4 Basic Networking

Let 'A' is user and 'B' is web server and we want to send data from A to B. It will require following steps:

4.1 How are machine and devices named?

IPv4 addressing and allocation:
IP adress are 32 bits unique address.
10000100 10101001 11100010 00000111
These 32 bits are partitioned into network bits and host bits.
Let network bits=25bits and host bits=7bits.Then, each network can have:
$2^7 = 128$ different host under it.

4.2 How 'A' discover 'B' name?

1. DNS[Domain Name Service]:
   DNS is a host name to IP address translation service. It translates human readable domain names (for example, www.google.com) to machine readable IP addresses (for example, 192.0.2.44).

4.3 How does'A' find path to 'B'?

Routing:
Routing is a process which is performed by network layer devices in order to deliver the packet by choosing an optimal path from one network to another.
In general,optimal path is shortest path with high bandwidth.

1. Inter-AS routing:
   - In this Routing, routing takes place between the autonomous networks.
   - BGP(Border Gateway Protocol) .
2. Intra-AS routing:
   - In this Routing, routing takes place within an autonomous network.
   - RIP(resource information protocol) and OSPF(open shortest path first).

4.4 How does 'A' send data to 'B'?

TCP(Transmission Control Protocol):

- It connection-oriented, and a connection between client and server is established before data can be sent.
- Reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender.
- Employs network congestion avoidance.
- Provides flow control and quality of service.

Each machine have 16 bits of Port number.
For application point of view ,machine address is "IP address+Port Number".

5 Conclusion

The basics of computer network communication include IP addressing,address translation through DNS,Routing and sending data through TCP.Each layer in network layer model has various functions and protocols that determine the rules of how communication in network is going to take place.Computer network security deals to make this communication secure.