Internet Infrastructure

One of the greatest things about the Internet is that nobody really owns it. It is a global collection of networks, both big and small. These networks connect together in many different ways to form the single entity that we know as the Internet. In fact, the very name comes from this idea of interconnected networks. The heart of the Internet exists between this telecommunications component and the content that users send to each other across those wires. That is what we call the Internet's 'infrastructure'. Internet infrastructure is the physical hardware, transmission media, and software used to interconnect computers and users on the Internet. Internet infrastructure is responsible for hosting, storing, processing, and serving the information that makes up websites, applications, and content.

7.1 BASIC SECURITY PROBLEMS

Cybersecurity is a daily concern in our personal and professional lives. When you go online, whether it's to shop, connect with friends and colleagues, or access an account, you worry about who might be tracking you or breaking into your files. Some of the basic security problems are as follows:

7.1.1 Code Injection

Hackers are sometimes able to exploit vulnerabilities in applications to insert malicious code. Often the vulnerability is found in a text input field for users, such as for a username, where an SQL statement is entered, which runs on the database, in what is known as an SQL Injection attack. Other kinds of code injection attacks include shell injection, operating system command attacks, script injection, and dynamic evaluation attacks. Attacks of this type can lead to stolen credentials, destroyed data, or even loss of control over the server.

There are two ways to prevent code injection: avoiding vulnerable code and filtering input. Applications can guard against vulnerable code by keeping data separate from commands and queries, such as by using a safe API with parameterized queries.

7.1.1 Data Breach

The cost of data breaches is well documented. They are often caused by compromised credentials, but the range of other common causes include softwaremisconfiguration, lost hardware, or malware (more on that below). Data breach prevention requires a range of good practices. Site traffic and transactions shouldbe encrypted with SSL, permissions should be carefully set for each group of users, and servers should be scanned. Employees should be trained in how to avoid beingcaught by phishing attacks, and how to practice good password hygiene. The principle of least privilege is worth noting here, as well.

7.1.2 Malware Infection

Most businesses are aware on some level of the security threat posed by malware, yetmany people are unaware that email spam is still the main vector of malware attack. Because malware comes from a range of sources, several different tools are needed for preventing infection. A robust email scanning and filtering system is necessary, as are malware and vulnerability scans. Like breaches, which are often caused bymalware infection, employee education is vital to keep businesses safe from malware.

Any device or system infected with malware must be thoroughly scrubbed, which means identifying the hidden portions of code and deleting all infected files before they replicate. This is practically impossible by hand, so requires an effective automated tool.

7.1.3 Distributed Denial Service of attack

A Distributed Denial of Service (DDoS) attack generally involves a group of computers being harnessed together by a hacker to flood the target with traffic. One of the most worrying aspects of DDoS attacks for businesses is that without even being targeted, the business can be affected just by using the same server, service provider, or even network infrastructure.

If your business is caught up in a DDoS attack, put your disaster recovery plan into effect, and communicate with employees and customers about the disruption. A security tool such as a WAF is used to close off the port or protocol being saturated, in a process which will likely have to be repeated as attackers adjust their tactics.

7.2 ROUTING SECURITY

Routing is fundamental to how the Internet works. Routing protocols direct the movement of packets between your computer and any other computers it is communicating with. By ensuring that packets go where they are supposed to, routing has a central role in the reliable function of the Internet. It ensures that emails reach the right recipients, e-commerce sites remain operational, and e- government services continue to serve citizens. The security of the global routing system is crucial to the Internet's continued growth and to safeguard the opportunities it provides for all users.

Every year, thousands of routing incidents occur, each with the potential to harm user trust and handicap the Internet's potential. These routing incidents can also create real economic harms. Key services may become unreachable, disrupting the ability of companies and users to participate in e-commerce. Or packets may get diverted through malicious networks, providing an opportunity to spy on them. While known security measures can address many of these routing incidents, misaligned incentives limit their use.

All stakeholders including policymakers, must take steps to strengthen the security of the global routing system. This can only be done while also preserving the vital aspects of the routing system that have enabled the Internet to be so ubiquitous and improving their security. Through leading by example in their own networks, strengthening communication, and helping realign incentives to favor stronger security, policymakers can help improve the routing security ecosystem.

There are three major types of routing incidents:

- **Route/prefix hijacking,** where a network operator or attacker impersonates another network operator, pretending that it is the correct path to the server or network being sought on the Internet.
- **Route leaks,** are the propagation of routing announcements beyond their intended scope (in violation of their policies).
- **IP spoofing,** where someone creates IP packets with a false source IP address to hide the identity of the sender or impersonate another system.

These incidents can create a serious strain on infrastructure, result in dropped traffic, provide the means for traffic inspection, or even be used to perform domain name server (DNS) amplification attacks, or other reflective amplification (RA) attacks.

The Mutually Agreed Norms for Routing Security (MANRS) is a set of visible, baseline

practices for network operators to improve the security of the global routingsystem.

Despite the availability of solutions to common routing incidents, ecosystem challenges limit their use.

- **Routing incidents are hard to address far from the source and must instead be addressed collectively.** Wherever a threat is coming from, the networks

  closest to its origin are best positioned to address the threat (e.g. adjacent networks can refuse to accept false announcements). When a network is impacted further from the source of a routing incident, it can only attempt tomitigate the impact. It must rely on other networks closer to the source of therouting incident to fully address the problem.
- **Economic externalities.** Any network can be the source of an incident and the insecurity of one network can impact all other networks. However, even if a routing incident originates from one's own network, the impact is most likelyto be felt on another network. Network operators are less likely to spend resources on better routing security since the benefits will mostly go to othernetworks, not their own.
- **Routing security is not a market differentiator.** Good routing security is currently not an effective marketing tool for network operators. It is difficultfor network operators to communicate their level of routing security to their customers. Users have limited understanding of the global routing system andhow their network's routing security practices will impact them.

  To improve routing security, we should:

  i. **Lead by Example.** All stakeholders, including governments, should improve infrastructure reliability and security by adopting best practices in their own networks.
     - All networks providing internet connectivity, including enterprise or government networks, should use filtering, alongside IP source validation, to help prevent and mitigate the impact of incidents.
     - In addition, influential market players, such as large enterprises or governments, should, where feasible, require compliance with routing security baselines, such as the one documented by MANRS, for procurement contracts with Internet service providers. MANRS, through its MANRS Observatory, will provide measurements that can serve as avaluable 3rd party assessment of a network operator's security practices.These assessments can help inform procurement decisions.

  ii. **Facilitate/encourage the adoption of common practices for routing security.** Industry associations, in close collaboration with governments and other stakeholders, should promote common baseline for routing security.
     - Common baseline for network operators provide an industry standard for routing security and promote greater information sharing among network operators. They also provide a method for network operators to signal their level of security to prospective customers.
     - All stakeholders can contribute to the adoption and development of common baseline and industry practices for routing security by participating in the development process and, where feasible, through funding.

  iii. **Support efforts to develop new, or strengthen existing, routing securitytools.** To further improve the security of the global routing system partnerships with the research community could help develop the next generation of routing security tools and practices.

- Where feasible, stakeholders, including governments and the private sector, can increase funding for research, development and experimentaldeployment of the next generation of Internet protocols, including thoseimproving routing security.
- Researchers can develop technical guidance on performing IP source validation, effective filtering, and global validation. Guidance should also encourage network operators to implement BGPSecand RPKI.

iv. **Encourage the use of security as a competitive differentiator.** To makerouting security a competitive differentiator, stakeholders should supportpublic awareness of the importance of routing security and encourage improved signaling of routing security between industry and customers.
- For Internet service providers, routing security is a core component of their overall security posture. Signaling their attitude towards routing security reflects strongly on their overall posture, which can differentiatetheir services from competition.
- Enterprises will pay more for better routing security, however they needways to determine good routing security from bad routing security. In a2017 survey, 94% of enterprises indicated that they would be willing topay more for a vendor who was a MANRS member in a competitive situation. The same research also found that awareness of MANRS was marginal among enterprises before the survey.
- Industry, consumer groups, governments and other stakeholders should worktogether to promote the use of routing security baselines, such as MANRS, as a competitive differentiator. In addition, they should support efforts to educate local enterprises about routing security and existing best practices.

v. **Strengthen communication and cooperation between network operators and other stakeholders.** Stakeholders should support the development of better mechanisms for information sharing, engage in information sharing on routing security, and collaborate with stakeholdersto address routing security threats.
- The private sector, governments, civil society, academia and others cansupport the development or strengthen existing computer security incident response teams (CSIRTs). CSIRTs provide an important role in information sharing and coordination in response to routing incidents and threats.

vi. **Identify and address legal barriers to information sharing, the implementation of routing security technologies and research onrouting incidents and threats.** Legal barriers can impede security researchers and disincentivize network operators from deploying routing security solutions and sharing information with one another.
- Identifying and eliminating legal and regulatory barriers can improve information sharing and responses to routing incidents. Stakeholders, particularly security researchers, may worry that disclosing routing security incidents or threats could place them in legal jeopardy. Legal barriers can also impede the development and deployment of routing security technologies. In developing solutions to identified barriers, stakeholders must pay close attention to their potential impact on the privacy of individuals.

7.3 WEAKNESS OF INTERNET SECURITY

Internet security is a broad term that refers to the various steps individuals and companies take to protect computers or computer networks that are connected to the Internet. One of the basic truths behind Internet security is that the Internet itself is not a secure environment.

The Internet was originally conceived as an open, loosely linked computer network that would facilitate the free exchange of ideas and information. Data sent over the Internet—from personal e-mail messages to online shopping orders—travel through an ever-changing series of computers and network links. As a result, unscrupulous hackers and scam artists have ampleopportunities to intercept and change the information. It would be virtuallyimpossible to secure every computer connected to the Internet around the world, so there will likely always be weak links in the chain of data exchange.

Due to the growth in Internet use, the number of computer security breaches experienced by businesses has increased rapidly in recent years. At one time, 80 percent of security breaches came from inside the company. But this situation haschanged as businesses have connected to the Internet, making their computer networks more vulnerable to access from outside troublemakers or industry spies.

7.3.1 Common Security Problems

Hackers have two main methods of causing problems for businesses' computer systems: they either find a way to enter the system and then change or steal information from the inside, or they attempt to over-whelm the system with information from the outside so that it shuts down. One way a hacker might entera small business's computer network is through an open port, or an Internet connection that remains open even when it is not being used. They might also attempt to appropriate passwords belonging to employees or other authorized usersof a computer system. Many hackers are skilled at guessing common passwords, while others run programs that locate or capture password information.

Another common method of attack used by hackers is e-mail spoofing. This methodinvolves sending authorized users of a computer network fraudulent e-mail that appears as if it were sent by someone else, most likely a customer or someone elsethe user would know. Then the hacker tries to trick the user into divulging his or her password or other company secrets. Finally, some hackers manage to shut downbusiness computer systems with denial of service attacks. These attacks involve bombarding a company's Internet site with thousands of messages so that no legitimate messages can get in or out.

7.3.2 Means of protection

Computer experts have developed ways to help small businesses protect themselvesagainst the most common security threats. For example, most personal computers sold today come equipped with virus protection. A wide variety of antivirus softwareis also available for use on computer networks. In addition, many software companies and Internet Service Providers put updates online to cover newly emerging viruses.

One of the most effective ways to protect a computer network that is connected tothe Internet from unauthorized outside access is a firewall. A firewall is a hardware security device that is installed between a computer network and the Internet. It acts like a Web server, routing traffic, but also blocks external users from accessing the internal computer system. Of course, a firewall cannot protect information once it leaves the network. A common method of preventing third parties from capturingdata while it is being transmitted over the Internet is encryption. Encryption programsput data into a scrambled form that cannot be read without a key.

There are several methods available to help small businesses prevent unauthorizedaccess to their computer systems. One of the most common methods is authenticationof users through passwords. Since passwords can be guessed or stolen, some companies use more sophisticated authentication technologies, such as coded ID cards, voice recognition software,

retinal scanning systems, or handprint recognitionsystems. All of these systems verify that the person seeking access to the computer network is an authorized user. They also make it possible to track computer activity and hold users accountable for their use of the system. Digital signatures can be used to authenticate e-mails and other outside documents. This technology providesproof of the origin of documents and helps prevent e-mail spoofing.

7.4 FIREWALLS

A firewall is a system designed to prevent unauthorized access to or from a privatenetwork. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet (the local network to which you are connected) orWAN must pass through the firewall (Fig. 7.1), which examines each message andblocks those that do not meet the specified security criteria.

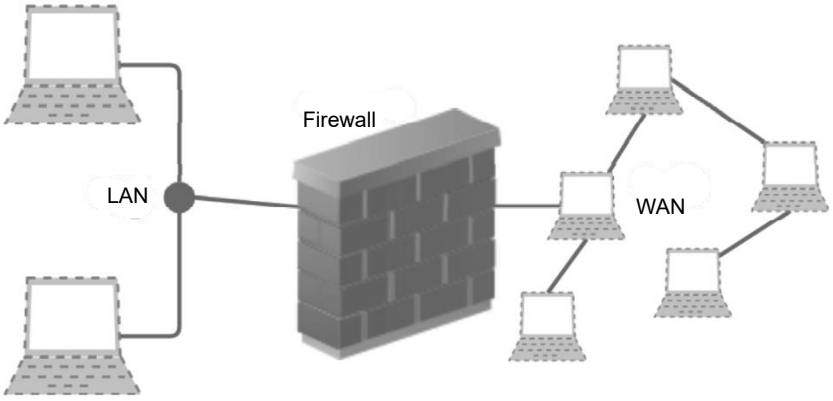

Fig.7.1: Illustration of Firewall

Firewalls need to be able to perform the following tasks:

- Defend resources
- Validate access
- Manage and control network traffic
- Record and report on events
- Act as an intermediary

7.4.1 Types of Firewalls

i. **Packet filtering:** The system examines each packet entering or leaving thenetwork and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

ii. **Circuit-level gateway implementation:** This process applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

iii. **Acting as a proxy server:** A proxy server is a type of gateway that hides thetrue network address of the computer(s) connecting through it. A proxy serverconnects to the internet, makes the requests for pages, connections to servers,etc., and receives the data on behalf of the computer(s) behind it. The firewallcapabilities lie in the fact that a proxy can be configured to allow only certaintypes of traffic to pass (for example, HTTP files, or web

pages). A proxy server has the potential drawback of slowing network performance, since it has to actively analyse and manipulate traffic passing through it.

iv. **Web application firewall:** A web application firewall is a hardware appliance, server plug-in, or some other software filter that applies a set of rules to a HTTP conversation. Such rules are generally customized to the application so that many attacks can be identified and blocked.

7.4.2 How Firewalls work?

Firewall match the network traffic against the rule set defined in its table. Once therule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like systemadministrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All thesetypes have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.