Technologies for Network Security

[1]D.Gokila MCA.,, [2]K.BrindhaMCA.,M.phil, [3]S.Balasubramani M.ScM.phil
[1]Assistant Professor , [1]Assistant Professor, [1]Assistant Professor
Department of Computer Science
[1]Sri Krishna Adthiya College of Arts and Science, Country.

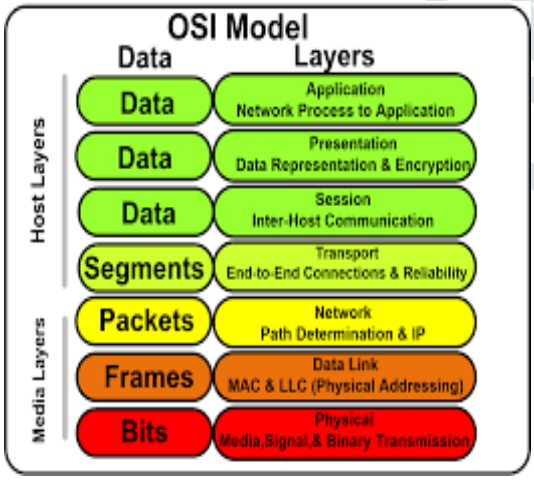
Abstract : Networking is the process of interconnection of nodes with each other. When the data is being transmitted around the pool of users there are chances of hacking the data and the data can be made as encrypted before reaching the customer.To avoid these there are allowing some of the techniques that is to be used while transmitting the data .In this aspect we discuss about the security measures to be used in providing the security to the data . We shall use software for preventative measures to protect the underlying **networking** infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a **secure** platform for computers, users,When the unauthorized users enter into the pool we shall the have signal and the data can be protected

***IndexTerms* – Cloud Secutiy, Web Security, Intrusion System, Security Information System.**

I. INTRODUCTION

Network is a dedicated link through data transfers from peer to peer. A computer network is a whole of connected computers. Computers on a network are called nodes. The link between computers can be done most commonly the internet cable, or wireless through radio waves. Linked computers can share resources like access to the Internet, printers, file servers, and others. A network is a multipurpose connection which allows a single computer can do more.

Network in the OSI Layers consists of seven layers each of which provides a transformation when travelling from one to other .When the data is converted as segments,Frames and packets there are chances of data lost when transmission



Networking Security Applications:

Some of the measure for the network security

Computer access control.

Defence in Depth.

Application security. Antivirus software. Secure coding. Secure by default. Secure by design. Secure operating systems.

Authentication. Multi-factor authentication.

Authorization.

Data-centric **security**.

Encryption.

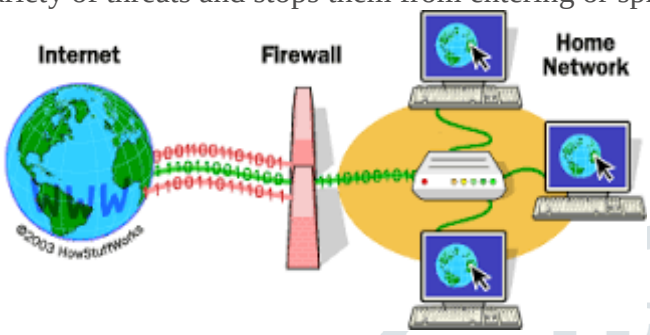
Firewall.

Firewall Security:

Firewall security plays the major role in providing the security to the internet . Firewalls put up a barrier between your trusted internal ***network*** and untrusted outside ***networks***, such as the Internet. ***Network*** segmentation. Antivirus and antimalware software. Access control. ***Application security***. Behavioral analytics. Data loss prevention. Email ***security***. Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.



Cloud based security systems:

"**Cloud**" data is stored on hard drives (much the way data is usually stored). And yes, it's probably more **secure** than conventionally stored data. ... Each of these companies has **cloud computing systems** — computer servers and storage devices, connected with computer networking equipment — that span the globe. Security poses a major challenge to the widespread adoption of **cloud computing**, yet an association of cloud users and vendors sees the cloud as a provider of information security services.

The Security-as-a-Service Working Group of the Cloud Security Alliance, a not-for-profit association formed by cloud-computing stakeholders, issued a **report** Monday that defines 10 categories of security services that can be offered over the cloud.

The alliance said its report is aimed at providing cloud users and providers greater clarity on security as a service in order to ease its adoption while limiting the financial burden security presents to organizations. The 10 security-as-a-service categories are:

1. **Identity and Access Management** should provide controls for assured identities and access management. **Identity and access management** includes people, processes and systems that are used to manage access to enterprise resources by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution.

2. **Data Loss Prevention** is the monitoring, protecting and verifying the security of data at rest, in motion and in use in the cloud and on-premises. **Data loss prevention** services offer protection of data usually by running as some sort of client on desktops/servers and running rules around what can be done. Within the cloud, data loss prevention services could be offered as something that is provided as part of the build, such that all servers built for that client get the data loss prevention software installed with an agreed set of rules deployed.

3. **Web Security** is real-time protection offered either on-premise through software/appliance installation or via the cloud by proxying or redirecting web traffic to the cloud provider. This provides an added layer of protection on top of things like AV to prevent malware from entering the enterprise via activities such as web browsing. Policy rules around the types of web access and the times this is acceptable also can be enforced via these **web security** technologies.

4. **E-mail Security** should provide control over inbound and outbound e-mail, thereby protecting the organization from phishing and malicious attachments, enforcing corporate policies such as acceptable use and spam and providing business continuity options. The solution should allow for policy-based encryption of e-mails as well as integrating with various e-mail server offerings. Digital signatures enabling identification and non-repudiation are features of many cloud e-mail security solutions.

5. **Security Assessments** are third-party audits of cloud services or **assessments** of on-premises systems based on industry standards. Traditional security assessments for infrastructure and applications and compliance audits are well defined and supported by multiple standards such as NIST, ISO and CIS. A relatively mature toolset exists, and a number of tools have been implemented using the SaaS delivery model. In the SaaS delivery model, subscribers get the typical benefits of this cloud computing variant elasticity, negligible setup time, low administration overhead and pay-per-use with low initial investments.

6. **Intrusion Management** is the process of using pattern recognition to detect and react to statistically unusual events. This may include reconfiguring system components in real time to stop/prevent an intrusion. The methods of intrusion detection, prevention and response in physical environments are mature; however, the growth of virtualization and massive multi-tenancy is creating new targets for intrusion and raises many questions about the implementation of the same protection in cloud environments.

7. **Security Information and Event Management** systems accept log and event information. This information is then correlated and analyzed to provide real-time reporting and alerting on incidents/events that may require intervention. The logs are likely to be kept in a manner that prevents tampering to enable their use as evidence in any investigations

Scope and Future Work

In the computer world today, client-server system has become popular because it is being used virtually every day for different applications. Some of the standardized protocols that client and servers use to communicate with themselves include: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP). Client-server system can be define as a software architecture made up of both the client and server whereby the clients always send requests while the server responds to the requests sent. Client-server provides an inter-process communication because it involves the exchange of data from both the client and server whereby each of them performs different function.

So security plays an important aspect The network **needs security** against attackers and hackers. Network **Security** includes two basic securities. The first is the **security** of data information i.e. to protect the information from unauthorized access and loss. And the second is computer **security** i.e. to protect data and to thwart hackers. The future can be systems which can be implemented

Conclusion

The market of network and security technology is one the rise with companies become more conscious of incoming and outgoing packets across the network barrier. Malware has been one of the most effective ways for hackers to intrude into the network security of companies. They are often bundled with other programs or attached as macros to incoming files. Vulnerability in an operating system and software also lead to systems being infected by malware.

With many people leaving their computer running on a continuous basis, there is an increased chance of the attack by memory-resident malware that are difficult to be detected forensically.

Reference links:

https://www.quora.com/Whats-the-future-of-network-security
https://www.sciencedirect.com/topics/engineering/network-technology
https://learn.org/articles/What_is_Networking_Technology.html
http://www.currenttech.net/networking
http://ecomputernotes.com/computernetworkingnotes/network-technologies
https://blogs.cisco.com/enterprise/the-5-technologies-that-will-change-networking-in-2019