PROJECT REPORT SUBMITTED FOR THE PARTIAL FULFILMENT OF THE

REQUIREMENT FOR THE AWARD FOR THE DEGREE OF

BACHELOR OF COMMERCE

BY

G.VEERA MANIKANTA III B.Com(Voc)

UNDER THE GUIDENCE OF

Smt. B.RANI DURGA, M.Com

Sri. P.V.RAMESH BABU , M.C.A

S.CH.V.P.M.R. GOVT DEGREE COLLEGE, GANAPAVARAM

DEPARTMENT OF COMMERCE

2021-2022

S.CH.V.P.M.R. GOVT DEGREE COLLEGE, GANAPAVARAM

DEPARTMENT OF COMMERCE

PROJECT NAME : INTERNET SECURITIES

CERTIFICATE

This is to certify that G.veera...manikanta of class IIIrd..b.com has successfully completed his/her project on topic .Internet....securities................. as prescribed by Mr..P.V...Ramesh....babu........during the academic year...2022............. as per the guidelines given by..head.....of.....Department.

Sign of external

Sign

Lecturer's name

(   )

INDEX

Introduction to Internet security.

Internet security is a branch of Computer security. it encompasses the Internet. browser security. web site security and network security as it applies to other application or operating system as a whole. Its objective is to establish rules and measures to use against attack over the Internet.

E-Commerce security is the guildeline that ensures safe transactions through the Internet. It consists of protocols that safeguard people who engage in online selling and buying goods and services.

Network security protect your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hard ware and software solutions as well as processes or rules and configuration relating to network use, accessibility and overall threat protection.

Network security involves access control, virus and antivirus software, application security, network analytics, types of network-related security [endpoint, web, wireless] firewalls, VPN encryption and move

Different types of Network security devices and tools.

* Access control
* Antivirus and anti-malware software.
* Application security.
* Behavioral analytics.
* Data loss prevention.
* Distributed denial of service prevention.
* mobile device security
* network segmentation.

* Access controls.

This refers to controlling which user have access to the network or especially sensitive section of the network. using security Policies. you can restrict network access to only recognized users and devices or grant limited access to non compliant devices or guest users.

* Antivirus and anti malware software.

malware or "malicious software" is a common form of cyberattack that comes in many different shapes and sizes.

Some variations work quickly to delete files or corrupt data. while other can lie dormat for long Period of time and quietly allow hackers a back door into your system.

* Data loss Prevention

Data loss Prevention [DLP] technologies are those Prevent an organization empolyee from sharing valueble company information or sensitive data - whether unwittingly or with ill intent outside the network. DLP technologies can prevent action that could potentially Expose data to bad actors outside the networking environment. such as uploading and downloading files, forwarding meassage or printing.

* Distributed denial of service Prevention.

Distributed denial of service [DDoS] attacks are becoming increasingly common. They function by overloading a network with one-side connection request that eventually cause the network to crash. A DDoS Prevention tools scrubs incoming traffic to remove non legitimate traffic that could threaten your network. and way conist of a hardware appliance.

* Application security.

Each device and software product used within your networking environment offers a potential way in for hackers. For this reason, it is important that all program be kept up to date and patched to prevent cyberattacker from exploting vulnerabilities to access sensitive data. Application security refers to the combination of hardware, software and best practies

* Behavioral analytics.

In order to identify abnormal behaviours, security support Personnel need to establish a baseline of what constitutes normal behaviours for a given customer users, Application and network. Behavioral analytics software is designed to help identy common indicatours of abnormal behavior.

* mobile device security.

The vast majority of us have mobile devices that carry some form of Personal or sensitive data we would like to keep protected. This is afact that hacker are aware of and can easily take advantage of implementing mobile deevice security measu can limit device access to a network which is ~~aness~~ anecessary step to ensuring network traffic stay Private and doesn't leak out through vulnerable mobile connection.

* Network segmentative.

Dividing and sorting network traffic based on certain classification streamlines job for security support Personal when it comes to applying Policies.

Needs for Internet security.

* Today, Internet is stuffed with different types of sensitive data.

* Today The Internet is packed with threats from hacker. They can.

- crash your system
- Acquire access to your personal information and can result in monetary lossers

so..,

* you need Interest security to keep information and system safe from malicious software and individals.

Threats

Malicious software.

* malware, a portmanteau of malicious softwa is any software used to disrupt computer operation gather sensitive information, or gain access to private computer systems.

* A botnet is a network of computers that have been taken over by a robot or bot that perform large-~~sacle~~ scale malicious acts for its creator.

* computer viruses are programs that can replicate their structures or effects by infecting other files or structues on a computer.

* Ransomware is a type of malware that restricts access to the computer system that it infects, and demands a ransom in order for the restriction to be removed.

Denial - of - service attacks.

A denial of service attacks [Dos] or distributed denial of serivice attack [DDos] is an attempt to make a computer resource unavailable to its intended users. It works by making so many serivice requests at once that the system is overwhelmed and becomes unable to process any of them. Dos may target cloud computing system. According to business participants in an international security servey. 25% of respondents experienced a Dos attack in 2007 and another 16.8% in 2010. Dos attacks often use bots to carry out the attack.

Phishing.

Phishing targets online user in an attempt to extract sensitive information such as Password and financial information. Phishing occurs when the attacker Pretends to be a trustworthy entity. either via email or a web Page. victims are directed to web Pages that appear to be legitmate. but instead route information to attacker. Tactics such as email spoofing attempt to make emails appear to be from legitimate senders or long complex URLs hide the actual web-site. Insurance group RSA claimed that Phishing accounted for worldwide losses of $10.8 billion in 2016.

Application vunlnerabilities.

Applications used to acess Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. Such bugs can give network attacker full control over the computer.

A widespread web-browser application vunerabitity is the cross orgin resource shoring [cors] vulnerability for maximum security and privacy, make sure to adopt adequate counter-measures againt it.

counter measures.

Network layer security.

TCP / IP protocoss may be secured with cryptographic methods and security protocols These protocols includes secure sockets layer [SSL] , suceded by Transport Layer security [TLS for web traffic Pretty Good privacy [PGP] for email . and IPsec for the network layer security.

Internet Protocol security.

Ipsec is designed to protect TCP /IP Communication in a secure manner . It is a se of security extension developed by the Internet Engineering Task Force [IETF]. It provides security and authentication at the IP layer by transforming data using encrypti

.

multi- factor authentication.

multi-factor authentication [MFA] is an access control method ~~of~~ in which a user is granted access only after successfully presenting separate pieces of evidence to an authentication mechanism - two or more from the following categories: knowledge, possession, and inherence Internet resources, such as websites and email may be secured using this technique.

Security token.

some online site offer customer the ability to use a six-digit code which randomly changes every 30-60 seconds on a physical security token The token has ~~bult~~ built -in computations and manipulates number based on the current time This means that every thirty second only a certain array of number ovaliduta access The website in made aware of that device's serial number and knows the computation and correct time to verify the number.

After 30-60 seconds the device presents a new random six-digits number to log into the website.

Electronic mail security.

Background.

Email message are composed, delivered and stored in a multiple step process which starts with the message composition. when amessage is sent. it is tranformed into a standrad format according to RFC 2822.

Pretty Goods Privacy

Pretty Good Privacy provides confidentialit by encryping message to be transmitted or data files to be stored using an encryption algorit such as Triple Des or CAST-128.

- Digitally signing the message to ensure its integrity and confirm the sender identity.
- Encrypting the message body of an email messa to ensure its confidentlity.

message authentication code.

A message authentication code [MAC] is a cryptography method that uses a secret key. to digitally sign a message. This method outputs a MAC value that can be decrypted by the receiver. using the same secret key used by the sender.

Fire walls.

A computer firewall controls access to a single compter. A Network firewall controls access to an entire network. A firewall is a security device computer hardware or software that filters traffic and blocks outsider. It generally consists of gateway and filiter. firewalls can also screen network traffic and block traffic decemd unauthorized.

web security.

Firewalls restrict incoming and outgoing network Packets, only authorized traffic is allowed to Pass through it.

Firewalls create checkpoints between network and computer. Firewalls can block traffic based on ip sources and tcp port number They can also serve as the platform for ipsec using tunnel mode. firewalls can implement VPNs Firewalls can also limit network explouse by hiding the internal network from the public Internet.

Types of firewall.

* Packet filter.

A Packet filter Processes network traffic on a packet by packet basis. its main job is to filter traffic from a remote ip host. so a router is needed to connect the internal network to the internet.

* stateful packet inspection.

In a stateful firewall the circuit level gateway is a proxy server that operates at the network level of an open system inter connect

* Application -level gateway.

An Application level firewall is a third generation firewall where a proxy server operative at the very top of the OSI model. The IP suite application level. A network packet is forwarded only if a connection is established using a known protocols.

* Browser choice.

web browser market share predicts the share of hacker attcks . For Example Internet Explorer 6. which used to lead the market.

Benefits of network security.

* Builds trust. security for large system translates to security for every one.

* mitigates risk

* Protects proprietory information.

* Enables a more modern work places.

* Access control.

* Antivirus and anti malware software.

* Application security.

* Behavioral analyties.

Advantages of Internet security.

* cyber security will defend us from critical cyber-attacks.

* It help us to browse the safe website

* cyber security will defend us from hacks & virus.

* The Application of cyber security used in our pc needs to update every weak.

* Internet security process all the incoming & outgoing data on our computer.

* It help to reduce computer chilling & crashes.

* Gives us privacy.

Disadvantages of Internet security.

* It was Expensive ; most of the user can't afford this.

* A normal user can't use their properly requiring special expertise.

* lack of knowledge is the main problem

* It was not easy to use.

* It makes the system slower

* It could take hours to day to fix a breach in security.

Personal safety.

The growth of the internet gave rise to many important services accessible to any one with a connection. one of these important services is digital communication. while this service allowed communication with other ~~to~~ through the internet. this also allowed communication with malicious user while malicious users often use the internet for Personal gain, this may not be limited to finanical /material gain. This is especially a concern to Parents and children, as children are often target of there malicious users. common threats of these malicious ~~st~~ safety include Phishing, Internet scams, malware, cyberstalking, cyberbullying, online Predators and sextortion.

10 best Practies for Internet security.

1. Use secure Passwords.
2. Don't reuse Passwords
3. Be suspicious of External downloads and emails.
4. Keeps an eye on the news for security incidents.
5. Have a crisis management and response Plan.
6. Back up your data
7. Keep Software, Programs, and application up to date.
8. secure your wifi
9. wipe data from old technology completely
10. Install, register and renew a total antivirus antipyware, and firewall Package on every computer.

conclusion.

security in the Internet is implaving. The increasing use of the Internet for commerce is improving the deployed techology to protect the financial transaltion, Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread.

Thanking you

I am very much Thankful to you to submit my project on "Internet security." per the co-operation and support of the college principal sir Sri P.madhu Raju Garu.m.s.c mphd and commerce Department.

I shall be every graceful to the department of commerce and Express by gratitude to All the facility to department of commerce.

Thanking you sir

your faithfully.
G.veera manikanta

Place :- Ganapavaram.

Date :-