NETWORKING – PART 2

NETWORK SECURITY CONCEPTS
INTRODUCTION TO WEB SERVICES
E-COMMERCE

VINOD KUMAR VERMA, PGT(CS), KV OEF KANPUR & SACHIN BHARDWAJ, PGT(CS), KV NO.1 TEZPUR

Network Security Concepts

- 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.
- Threats to Network Security:
  - Virus
  - Worms
  - Trojan Horse
  - Spams

VIRUS

- Are the malicious code/programs that cause damage to data and files on a system.
- Virus attach itself to program or file so that it can spread from one computer to another leaving infection as it travels.
- Some Virus cause only annoying effects like changing desktop icons, etc. while others can damage your hardware, software or files.
- Almost all Virus are attached to an executable file, it means Virus cannot infect your computer unless you run or open the program/file.
- It means Computer Virus cannot spread without a human action.

Damage Caused by Virus

- **DAMAGE OR DELETE FILES** : some virus may delete or damage random documents or specific file that are crucial to Operating System and system will not be able to boot.
- It may slow down your computer
- **INVADE YOUR EMAIL PROGRAM:** some forms of viruses may wreak even more havoc by spreading themselves to the contact in your address book

Prevention from Virus

- Use Anti-Virus Software: scan all your computer for virus, disconnect infected PC from network, notify anti-virus vendor to update its database.
- Regularly update your Anti-Virus
- Don't download or open email from unknown sender
- Don't click on link in email rather type the link in address bar
- Disconnect the internet if you are away
- Disable cookie if possible

WORM

- A worm is a self-replication programs which eats up the entire disk space or memory. A Worm keeps on creating its copies until all the disk space or memory is filled.
- Worms harm to a computer or a computer network by consuming bandwidth and slow down the network speed. After the worm has infected a system, it can propagate to other systems via internet or while copying files from one system to another without user interaction

Damage caused by WORM and prevention

- DAMAGE
  - It eats up entire disk space or memory
  - Consumes network bandwidth and slows down the network speed.
- PREVENTION
  - Use Total Security software and scan the PC using the option BOOT TIME SCAN.
  - Update regularly
  - Avoid inserting infected pen drives

Trojan Horse

- Is a program that appears harmless (such as text editor or a utility program) but actually performs malicious functions such as deleting or damaging files.
- With help of Trojan, harm that could be done by hacker on target computer systems are:
  - Data theft
  - Installation of unwanted softwares
  - Keystroke logging
  - Downloading or uploading of files. And many more…

Prevention from Trojan Horse

- Use Total Security software
- Update regularly
- Never download any software of file from untrusted website
- While using public computer, check for any addition device connected to it or be alert of keylogger software, so for financial transaction prefer to use VIRTUAL KEYBOARD rather than keyboard typing
- Logout from your account and remove history if you are working on public computer

SPAMs

- Means sending of bulk-mail by an identified or unidentified source. In non-malicious form, bulk advertising mail is sent to many accounts. In malicious form (email bombarding) the attackers keeps on sending bulk mail until the mail-server runs out of disk space. Damages are:
  - ***Spam reduces productivity:*** *billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance and reduce overall productivity*
  - ***Spam eats up your time:*** *deleting spam emails like the simple solutions, but it eats a significant amount of productivity*
  - ***Spam can lead to worse things:*** *spam messages may contain offensive, fraudulent material and can even be used to spread viruses.*

Cookie

- Also known as web cookie or browser cookie, is a small piece of data sent from a website and stored in a user's web browser while a user is browsing a website. Some cookies disappear after user closes his browser while others, known as tracking cookies, remain saved and load the next time user visits the same website.
- Cookie help website to store information about visitors like username, password and other details.

Cookie

- Although cookie help track user's browsing sessions and load information faster, but create some security and privacy concerns as well. These security and privacy concerns are:
  - **Session Data:** When we visit any website on regular basis, we may not have to enter username and password to get in. That's because the information is being pulled from tracking cookie. These cookie stores information in encrypted form but if somebody gets the encryption key he could discover your password

Cookie

- **Tracking Information:** when you visit certain websites with advertisements, those ads create cookies that store and track your online pattern. You may have noticed that if you go to a clothing store's website, for example you'll see ads for that store when you click away to other website. That's because tracking cookies have relayed this information back to advertisers, who use it to target their ads.
- **Public Computers:** the same general threats exists for traffic cookies saved on public computer. So it is advised when you finish using public computer or shared computer, delete the cookies to ensures that the next people who use the same computer can't access the information

Firewall

- A firewall is a technique used in a secured computer system or network to block unauthorized access and allow only the authorized user.
- Firewalls can be implemented in either hardware or software, or a combination of both. It is a device or set of devices or software running on a computer, which is configured to permit or deny computer

Firewall

Software firewall	Hardware Firewall
Firewall softwares are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. It could also provide protection against the most common Trojan or Worms	It is physical piece of equipment designed to perform firewall duties. It may be actually be another computer or dedicated piece of equipment which serve as firewall. Firewall keep out malevolent hackers and people who intended to do damage and take over other peoples' servers.

HTTPS

- HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site.
- Users expect a secure and private online experience when using a website.
- We encourage you to adopt HTTPS in order to protect your users' connections to your website, regardless of the content on the site.

HTTPS

- Data sent using HTTPS is secured via *Transport Layer Security* protocol (TLS), which provides three key layers of protection:
- ENCRYPTION : encrypting the exchanged data to keep it secure from eavesdroppers. That means that while the user is browsing a website, nobody can "listen" to their conversations, track their activities across multiple pages, or steal their information.
- DATA INTEGRITY : data cannot be modified or corrupted during transfer, intentionally or otherwise, without being detected.
- AUTHENTICATION : proves that your users communicate with the intended website.

Closed Lock Pad (Secure Connection)

HTTPS

India IT Act

- The IT Act, 2000 is an Act of the Indian parliament (No. 21 of 2000) notified on 17 October, 2000. It is the primary law in India dealing with cybercrime and electronic commerce.
- The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The law apply to the whole of India.
- Persons of other nationalities can also be indicted under the law if the crime involves a computer or network located in India.

Common Section under IT Act

SECTION	OFFENCE	PENALTY
67A	Publishing images containing sexual acts	Imprisonments up to seven years or fine up to Rs. 10,00,000.
67B	Child pornography	Imprisonment – 5 years to 7 years Fine – 10,00,000
70	Securing access or attempting to secure access to a protected system	Imprisonment up to 10 years or fine

IT Act Amendments

- A major amendment was made to the IT Act in 2008.
- It introduced section 66A which penalized sending of offensive message.
- It also introduced section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource"
- The Act was passed in December 2008 and came into force in October 2009.

Cyber Law

- Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues.
- Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy.
- Generically, cyber law is referred to as the Law of the Internet.
- Cyber Law also called IT Law is the law regarding Information-technology including computers and internet.
- **Importance of Cyber Law:**
- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

Areas of Cyber Law

- Fraud
- Copyright
- Defamation
- Harassment and Stalking
- Freedom of Speech
- Trade Secrets
- Contracts and Employment Law

Cybercrime

- Is any criminal offense that is facilitated by, or involves use of electronic communications of information system including any electronic device, computer or the Internet.
- It involves the terms like : Phishing, Credit Card Frauds, illegal downloading, industrial espionage, child pornography, cyber bullying, cyber stalking, cyber terrorism, creation and /or distribution of viruses, spam and so on

Example of Cybercrime

- **CYBER TROLLS AND BULLYING**: It refers to a person who purposely post opposing, sarcastic, demeaning or insulting-comments about something or someone with an aim of targeting a person online. The provocative messages posted this way are also called trolls. It is a cyber crime and is a form of cyber bullying.
- **CYBER BULLYING:** Harassing, demeaning, embarrassing, defaming, or intimidating someone using modern technologies like internet, cell phones, instant messengers, social networks etc. is called Cyber Bullying.
- **CYBER STALKING:** It is a kind of online harassment wherein the victim is subjected to barrage of online messages and emails. Typically these stalkers know their victims instead of resorting to offline stalking, they use the internet to stalk, etc.

Reporting Cybercrime

- If any cyber crime happens, one must report it firstly to parents, school authorities and then to police.
  - The local police stations can be approached for filing complaints just as the cybercrime cells specially designation with the jurisdiction to register complaint
  - In addition, provisions have now been made for filing of E-FIR in most of the states
  - In addition, the ministry of Home Affairs is also launching a website for registering crimes against women and children online including cybercrimes

IPR issues

- It refers to Intellectual Property Rights.
- It refers to something owner has legal rights.
- This term became popular in context of computer ethics.
- Intellectual Property refers to creations of the intellect, inventions, literacy and artistic work, symbols, names, image and design used in commerce are part of it.
- It is divided into 2 categories:
- **INDUSTRIAL PROPERTY:** it includes inventions, trademark, design, commercial names, etc.
- **COPYRIGHT**: it includes literacy and artistic works such as novel, poems, film, story, drawing, painting, photograph. It is legal concept, enacted by most governments, giving the creator or original work exclusive rights to it, usually for a limited period.

Hacking

- The gaining of unauthorized access to data in a system or computer.
- Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system.
- Hacking is classified according to their intent:
  - Ethical Hacking
  - Cracking

Ethical Hacking

- Process to gain access to systems with a view to fix the identified weakness. They may also perform penetration testing and vulnerability assessments.

Cracking

- Refers to gain unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Introduction to Web Services

VINOD KUMAR VERMA, PGT(CS), KV OEF KANPUR &
SACHIN BHARDWAJ, PGT(CS), KV NO.1 TEZPUR

WWW

- Stands for World Wide Web also known as Web.
- It is a collection of website or web pages stored in web server and connected to devices through the Internet.
- These website may contain text, images, audio, sound, animation etc.
- The WWW, with Internet allows retrieval and display of website to your device.
- WWW was invented by Tim Berners Lee in 1989. *Internet and Hypertext as available at that time. but no one thought how to use the internet to link or share one document to another. Tim focused on three main technologies that could make computers understand each other, HTML, URL, and HTTP. So, the objective behind the invention of WWW was to combine recent computer technologies, data networks, and hypertext into a user-friendly and effective global information system.*

HTML

- Stands for Hypertext Markup Language
- Hypertext Markup Language is the standard markup language for documents designed to be displayed in a web browser.
- It is generally assisted by other technologies like CSS, JavaScript, AJAX etc.
- It is tag based code, where tags are predefined. Tags are the instruction how web page will appear on browsers.
- It is not case sensitive.
- HTML files are stored with extension .HTM or .HTML
- Few tags are: <HTML>, <TITLE>,<A>,<IMG> etc

XML

- Stands for extensible markup language
- Extensible Markup Language is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.
- It allows us to exchange data between heterogeneous system.
- XML stores information in a plain text format so it is not blocked by any firewall.
- Tags are not predefined i.e. we can create our own tag
- It is case sensitive.

Difference between HTML and XML

HTML	XML
It focuses on presentation of data i.e. how the data will appear on web page.	It focuses on structure of data i.e. how data is stored. XML data can be presented on web page by using XSLT (XML Style sheet Language Transformation)
TAGs are fixed i.e. we cannot create our own tag	TAGs are not fixed, we can create our own tag
Case Insensitive	Case Sensitive
Ordering of TAG is immaterial	Ordering of TAG i.e. nesting of TAG must be in correct order

HTTP

- Stands for Hypertext Transfer Protocol
- Used to transfer all files and other data(resources) from one computer to another on the world wide web.
- Client(Browser) send request to Web Server using HTTP protocol and Server respond back to Client using HTTP i.e. Client and server over web communicate using HTTP protocol.
- HTTP is stateless protocol, various technique applied to make HTTP as State full like Cookies.
- See the format of URL:
  - http://www.google.com

DOMAIN NAMES

- Communicating with computer on internet using IP address is practically impossible as it is very difficult to remember IP address of every computer or website.
- System has been developed to assign names to IP Address and maintains a database of these names corresponding to IP address.
- These names are referred as Domain Name.
- Example – **cbse.nic.in, gmail.com**
- It is used in URL(uniform resource locator) to identify particular web servers.
- Domain name has more than one parts –
  - Top Level Domain Name or Primary Domain Name
  - Sub Domain names
- For example in cbse.nic.in in is the primary domain, nic is sub domain of in and cbse is sub-domain of nic.

DOMAIN NAMES

Generic Domain Names:-

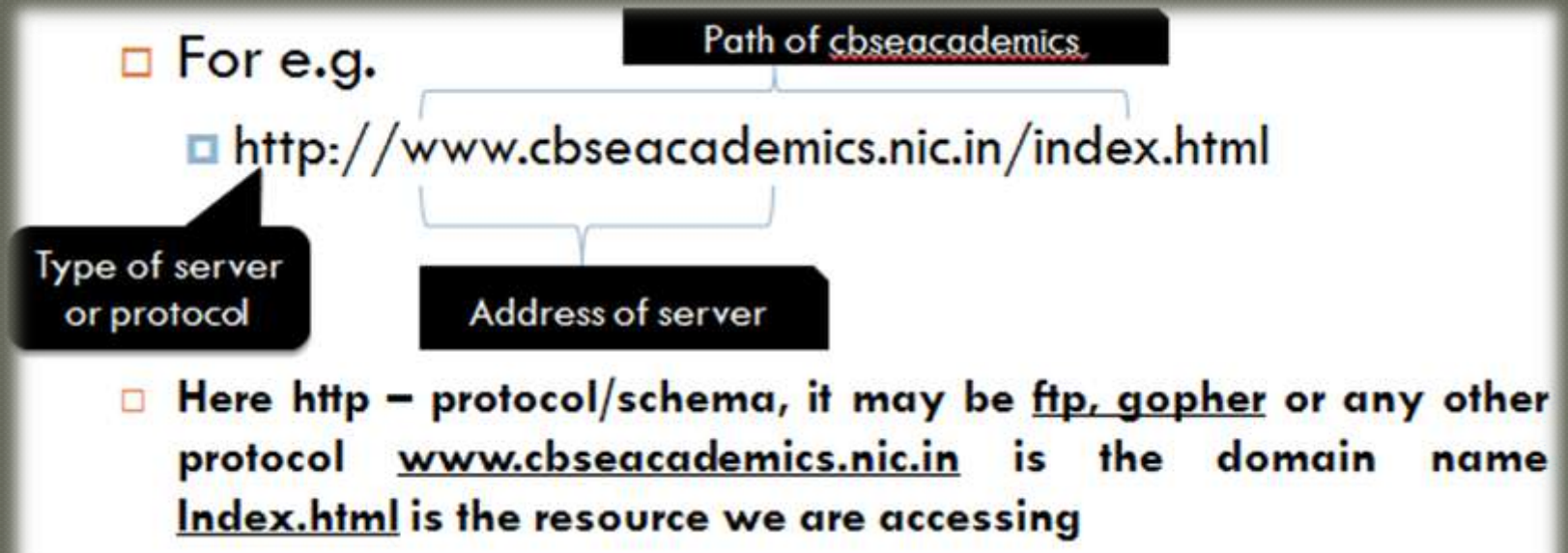
- ✓ .com – commercial business
- ✓ .edu – educational institutes
- ✓ .gov – government agencies
- ✓ .net network organizations
- ✓ .org Organizations(nonprofit)

Country Specific Domain Names:-

.in – india
.au – australia
.ca – canada
.ch – china
.nz – new zealand
.pk – pakistan
.jp – japan
.us – united states of America

URL

- Stands for Uniform Resource Locator.
- Each web site has a unique address called URL,
  for e.g. http://www.cbse.nic.in
- The basic format of URL is :
  type://address/path



Website

- A website is a collection of web pages and related content that is identified by a common domain name and published on at least one web server.
- For example: google.com, youtube.com
- All publicly accessible websites collectively constitute the world wide web.
- Website is broadly of two types:
  - **STATIC WEB SITE :** static web site is used to display information without any interaction with user or web server.
  - **DYNAMIC WEB SITE:** allows user interaction with web site and can communicate with web server again and again.

Web Browser

- A web browser is a software application for accessing information on the World Wide Web.
- Web Browser act as a client to send request to server, once web server process the request and returns the response the same will be displayed on web browser.
- There are many popular web browsers available like : Google Chrome, Firefox, UC Browser, Opera.
- Most of the Web Browser supports Graphical support, Lynx is the text based web browser

Web Servers

- A **web server** is a computer that runs websites
- It's a computer program that distributes **web** pages as they are requisitioned.
- The basic objective of the **web server** is to store, process and deliver **web** pages to the users.
- Web server and client communicate with the help of HTTP protocol.
- Web server returns the requested page to client with response code like 404 (if requested page not found), 200 (if requested page found) etc.

Web Hosting

- Is a service which allows individual or organization to make their web site accessible through world wide web.
- Web site is hosted on special computer called Web servers. If the site is hosted users can access the website from website from anywhere in the world.
- To Host a website, we require DOMAIN NAME, WEB SPACE.
- Web Hosting provides various services like – FTP upload, Email account, web site building tool, databases etc.

Web Scripting

- Without adding web scripting a web site is static.
- Is a programming language for adding dynamic capabilities to world wide web.
- Web scripting can be used for simple action like changing the button color when mouse is over on it or to complex thing like interactive online games.
- Dynamic content can be added to website using scripting. For e.g. if user fills a registration form, it is good practice to validate the entries.
- Web Scripting if of 2 type:
- CLIENT SIDE
- SERVER SIDE

Client Side Scripting

- Client side script executes on the web browser i.e. not interaction with the web server.
- It is generally used for performing action which do not require interaction with the server like: checking text field is empty, password is of certain length, password contains pattern of text, CAPTCHA validation, new password and confirm password is same or not.
- Client side scripting languages are : Java Script, VB Script, Action Script

Server Side Scripting

- This type of scripting execute on the web server i.e. when user clicks on any button or interactive object the request goes to server and executes on server and response comes to web browser.
- Server side scripting is used for the action like validating the username and password, availability of user id, submitting the information to store it in database etc.
- Popular server side scripting language are: ASP(Active Server page), PHP (PHP Hypertext preprocessor), JSP(Java Server Pages)

Web 2.0

- Web 2.0 is the name used to the describe the second generation of the world wide web, where it moved static HTML pages to a more interactive and dynamic web experience.
- Web 2.0 is focused on the ability for people to collaborate and share information online via social media, blogging and Web-based communities.
- Web 2.0 is pronounced web-two-point-o.
- Facebook, Wikipedia, Google Adsense, Twitter,etc are example of Web 2.0
- Popular technologies are: AJAX, JQuery, Silverlight, Flash etc.

E-Commerce payment

- When you purchase goods and services online, you **pay** for them using an electronic medium. This mode of **payment**, without using cash or cheque, is called an **e-commerce payment** system and is also known as online or electronic **payment** systems.
- Different types of e-commerce payment:
- Credit Card
- Debit Card
- Smart Card
- Net Banking
- E-Wallet
- Mobile Banking

Payment by Credit Card

- User pay by providing Card Number, Expiry date, Name of Card and CVN (Card verification Number). OTP is received on registered number for double verification i.e. for security reason

Payment by Debit Card

- User pay by providing Card Number, Expiry date, Name of Card and CVV (Card verification Value). OTP is received on registered number for double verification i.e. for security reason

VINOD KUMAR VERMA, PGT(CS), KV OEF KANPUR & SACHIN BHARDWAJ, PGT(CS), KV NO.1 TEZPUR

Payment by Net banking

- It is simple method of paying online from customer's bank account.
- User must logged in by providing username, password
- High security password or OTP is received for security reason and once entered and validated, payment is done.

Payment by Mobile banking

- In this customer has to download software provided by bank and linked it with the account. M-PIN is used for mobile banking.
- Customer can link Debit/Credit card with this software and make the payment.

VINOD KUMAR VERMA, PGT(CS), KV OEF KANPUR & SACHIN BHARDWAJ, PGT(CS), KV NO.1 TEZPUR

UPI

- Stands for Unified Payment Interface
- Developed by National payments corporation of India (NPCI) under the guidelines of RBI
- It allows to send and receive money between accounts linked with mobile number.
- The BHIM UPI app enables the users to link the app with the accounts where they have already linked the same mobile number. The sending and receiving of money are done on a real-time basis and it does not require the IFSC code. Instead of IFSC Code, both the sender and receiver need a VPA or Virtual Payment Address. The VPA is something like this yourname@sbi or yourname@icici etc.

UPI

- You can create several VPA using BHIM- UPI official android app or using any of the Indian Banks UPI apps and linked more than one Bank Account, only you have to link the same mobile number or SIM which you are using in your smartphone with your Bank Account. Because before creating VPA, the UPI payments app will verify your SIM by sending an SMS, to authenticate the linked Bank Account.

Payment Apps

- Popular payment apps(with wallet) are:
  - PayTM
  - PhonePay
  - Amazon Pay
  - Google Pay etc.