Topic 5
Web Security

Slides developed by

What you will learn in these slides...

- The Uniform Resource Locator
- HTTP Methods and CRUD
- Port Numbers
- HTTP Status Codes

The Internet and the World Wide Web

YouTube Link: https://www.youtube.com/watch?v=J8hzJxb0rpc

Uniform Resource Locator (URL)

- The URL is the address of a website or resource on the Internet
  - e.g., facebook.com, minecraft.net, singhealth.com.sg
- Every webpage on the Internet has a URL
- All URLs start with http:// or https:// although accessing a website may not require typing it in the search bar

An example of a URL

https://www.youtube.com/watch?v=jNQXAC9IVRw

How to read a URL

https://www.player.com:80/gamelist.php?key1=value1&key2=value2#RacingGames

Scheme Domain Name Port File Path Parameters Anchor

URLs consist of (in sequence):

Scheme	The protocol used to request for the source (usually http or https)
Domain Name	The website or web server that is requested. IP addresses may be used in place of domain names
Port	Port number used to access a resource. A colon separates the port from the domain name. If the protocol is http or https, the port is usually not included in the URL (port numbers will be discussed later in this topic)
File Path	Tells the browser to load a specific file or page on the website/web server. A URL with no specified path usually leads to the home page of the website
Parameters	A string of 'random' characters after the file path. Starts with a question mark. Often seen in URLs for browser searches or YouTube videos
Anchor	Acts like a bookmark for long webpages with multiple sections. Starts with a hashtag. Used to scroll to or load a specific page of the page

Do note, URLs need not contain all components

Reference: https://edu.gcfglobal.org/en/internetbasics/understanding-urls/1/

Recap on Topics 2 and 4

- In Topic 2, we learned various cyber threats, while in Topic 4, we dove deeper into malware-focused threats
- From these topics, how do we identify malicious websites?

Do not click on links in phishing emails

Check for typos in the URL, e.g., facebo0k.com / goog1e.com

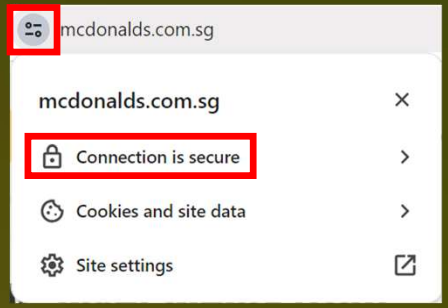
Check the properties of links by hovering over them

Use a website safety checker if you are unsure, such as Google Safe Browsing or VirusTotal

HTTP and HTTPS

Before we discuss HTTP status codes, let's go through the most common protocols used throughout the Internet, HTTP and HTTPS

HTTP	HTTPS
• Stands for Hypertext Transfer Protocol • Is the foundation of data communication on the World Wide Web • Transfers data from a web server to a web browser • Data sent via HTTP is not encrypted and is vulnerable to interception	• Stands for Hypertext Transfer Protocol Secure • An extension of HTTP with more secure features • Data sent via HTTPS is encrypted which is more secure and prevents interception • Clicking the icon next to the URL on a web browser's search bar will indicate if a connection is secure by displaying a padlock icon



HTTP Methods

- Specifies the desired action performed on a HTTP request
- There are 4 commonly used HTTP methods (aka verbs)

POST
Adds new data to a resource. Can also create new resources

GET
Retrieves data from a resource

PUT
Updates a resource with the request from the user

DELETE
Deletes the specified resource

- Other methods do exist (e.g., HEAD, OPTIONS, CONNECT, TRACE) but are out of scope from this topic

Reference: https://www.contrive.mobi/aviorapi/HTTPMETHODS.html

CRUD and its relation to HTTP methods

- Stands for Create, Read, Update, Delete
- They are operations which how explain the nature of an interaction between applications and data
- The 4 common HTTP methods follow the CRUD operations closely
  - POST -> Create
  - GET -> Read
  - PUT -> Update
  - DELETE -> Delete

HTTP methods in cyber awareness

HTTP methods have different security implications and can be exploited if not properly managed

Method	Importance	Potential Vulnerability
POST	POST requests send data in the body (data which is sent to the server), and this is often more secure than sending data in the URL.	SQL injection or Cross-site scripting may occur if there is no input validation in place.
GET	GET requests are read-only and the server state should remain unchanged.	Man-in-the-middle attack may occur when queries are sent through the search bar. Therefore, GET requests should not include sensitive information when requesting through a URL.
PUT	Proper authentication and authorization must be in place to prevent unauthorized parties from updating data.	Data can be overridden by attackers if authentication and authorization are not in place.
DELETE	Access control measures must be enforced to prevent unauthorized deletions.	Data loss can occur if it is not properly protected.

Port Numbers

- Identifies a specific process on a server (e.g., web server, email server, file transfer etc.)
- Numbers range from 0-65535
  - 0-1023: well-known ports
  - 1024-49151: registered ports
  - 49152-65535: dynamic/private ports (often used for testing)
- Most port numbers use the Transmission Control Protocol (TCP) and/or User Datagram Protocol (UDP)
- Some commonly used port numbers you should know

20, 21	File Transfer Protocol (FTP)	**TCP**
22	Secure Shell (SSH)	**TCP**
25	Simple Mail Transfer Protocol (SMTP)	**TCP**
53	Domain Name System (DNS)	**Both**

80	HTTP	**TCP**
123	Network Time Protocol (NTP)	**UDP**
443	HTTPS	**TCP**
3389	Remote Desktop Protocol (RDP)	**TCP**

Reference: https://www.techtarget.com/searchnetworking/definition/port-number

TCP vs UDP

TCP	UDP
• Connection-oriented (a connection is established between sender and receiver) • Ensure data is delivered accurately • Does error-checking and data will be re-sent if errors occurred • Used when reliability is crucial Examples where TCP is used • Web browsing • Email • File Transfer	• Connectionless • Does not do error-checking and therefore is not guaranteed that data is sent accurately • Faster due to lack of connection • Used when speed is prioritised Examples where UDP is used • Video streaming • Online gaming

HTTP Status Codes

- Three-digit response codes given by web servers on the Internet
- Defines the outcome of a client's request to a server

Status Code categories

1xx	Informational	Client request was received, and server is continuing to process it Example: 101 (Continue): Server received the request headers, and client should send the request body, such as a POST request
2xx	Success	Request was successfully received, understood, and accepted Example: 200 (OK): Request was successful, and server returned the requested resource
3xx	Redirection	Further action must be taken by the user agent to fulfill the request Example: 301 (Moved Permanently): Requested resource has been moved permanently to a new URL
4xx	Client Error	Client made an error with the request Example: 404 (Not Found): Requested resource could not be found on the server
5xx	Server Error	Server encountered an error while processing the request Example: 502 (Bad Gateway): Server received an invalid response from an inbound server it accessed while trying to fulfill the request

Status codes in cyber awareness

Enhance your awareness by learning important status codes and actions you can take!

Code	Name	Description and Actions Recommended
401	Unauthorized	• User must provide valid authentication credentials to access the requested resource • Educate users on the importance of strong passwords and encourage usage of MFA.
403	Forbidden	• Server understood the request, but the user is not allowed to access the resource • Educate users on access control policies and permissions. Ensure they understand why they may be denied access and the importance of adhering to the restrictions.
404	Not Found	• Requested resource could not be found on the server • Phishing attacks may lead to non-existent webpages, activating the 404 code, while secretly stealing or gaining access to confidential data. • Educate users on identifying legitimate URLs and avoid clicking suspicious links.
500	Internal Server Error	• Generic server error which often happens due to an unexpected condition • Educate users on potential security implications of server errors, such as vulnerabilities that can be exploited. Report any unexpected server errors to the IT department.
502	Bad Gateway	• Indicates various issues with the server • Educate users on the importance of maintaining server security. Update and patch systems regularly. • Implement rate limiting to set the maximum number of requests your webpage can handle at a time to prevent DoS attacks.
503	Service Unavailable	
504	Gateway Timeout	

VIGILANCEHUB
SECURE TODAY, THRIVE TOMORROW

Topic 5 Summary

- Safe web browsing practices
- The URL
  - Components that make up a URL
- HTTP Methods and CRUD
- Port Numbers
  - TCP and UDP
- HTTP Status Codes
  - Important codes to take note

In the next topic...

Network Security

- Networking fundamentals
- Network components
- Network monitoring practices