2.5 Browser-Based Crimes

Table 2.5 Browser-Based Attacks[2,3,6]

Browser attack	**What it is ?**
Browser Cache Poisoning	Collection of critical information from the browser cache.
Man-In-The-Middle attack	An active network attacker positions himself in the network between the victim and the targeted web application
Passwords in browser memory	Attacker can steal the stored login details of a user in a browser memory and escalate his privilege .
Back & Refresh attack	Collecting sensitive and important details by the use of Back button and the browser's Refresh feature.
Autocomplete	The attacker can easily get hold of saved password in the browser by unaware users.
Browser history	Leakage of sensitive information through the URL from the browser's history.
Cross-Site scripting	malicious script injection by attacker into a web page leading to a target.
CSRF	An attacker tricks a victim into performing actions on their behalf.
Eavesdropping attack	A passive or active network attacker listens in on other user's network traffic, such as DNS queries, HTTP requests and responses and the like.
UI Redressing	It is also known as clickjacking or tap jacking, redresses or "redecorates" a target application, confusing the user who is interacting with the application. Eg. such as clicking a button, dragging-and-dropping items, etc.
Session Hijacking	A session hijacking attack allows the attacker to transfer an authenticated session from the victim's browser to an attacker-controlled browser.
Session Fixation	It enables an attacker to force the victim's browser to use an existing session, which is also known by the attacker.
Social Engineering Attacks	It focuses on people as the attack vector, using psychological manipulation techniques to trick people into performing certain actions or into divulging confidential information

2.6 Types of Email Attacks

The most common types of Email Attacks are presented at Table 2.3

Table 2.3 Types of Email Attacks[8,9].

Phishing	Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions.One of the most common methods used by attackers to gain access to information is through the mass distribution of e-mail messages or social engineering. It may take various forms such as fictitious email meant to cause an emotional reaction such as worry, or surprise, that an order was placed by the recipient, the activity of fraudulently presenting oneself online as a legitimate enterprise in order to trick consumers into giving up personal financial information that will be used for identity theft or other criminal activity, attacker use a familiar word in the sending address to mimic a known entity and plays into a potential emotional reaction of wanting to investigate an unauthorized purchase. Web sites like xyz.com does not exist and a quick Google search will show that it is a scam, message looks very casual and personable, something that a real person would send. The attacker also leveraged the use of the "specific word " in the email address which can play upon the receiver's habit of looking for "specific word.", well-designed attack meant to mirror an invite from a well-known professional networking site and attacker used a familiar word in the sending address to mimic a known entity. It also plays into a potential emotional reaction of wanting to investigate an unauthorized purchase
spear-phishing	Before sending the email, the criminal observe the target's interests and delivers personalized emails to a single individual.
Smishing	Smishing is phishing using text messaging on mobile phones to gain the trust of the victim. For example, a smishing attack might send the victim a website link.
Whaling	Whaling is a phishing attack that targets high profile targets within an organization such as senior executives. Additional targets include politicians or celebrities
Pharming	Pharming is the impersonation of a reputable website to dupe individuals to submit their personal information.
Spyware	It is software that allows a criminal to collect data about a user's computer activity. Activity trackers, keystroke collecting, and data capture are all standard features of spyware.
Scareware	Scareware creates pop-up windows generating the fake message to encourage the user to execute a specified action or to execute a specific program.
Adware	Adware is a malware which track the pages visited by the user to know users intrest. It can then send relevant pop-up advertisements to those websites and generates cash for

	its makers by displaying unpleasant pop-ups on the visited web site.
Spams	Spams are Unsolicited emails/junk emails which contain hazardous links, viruses, or false content. to collect sensitive data from the infected computers.
Vishing	A vishing attack can be conducted by voice communication such as voice email, smartphone, VoIP (voice over IP), or landline phone and criminals can fake calls from legitimate sources in which individuals are tricked over the phone into revealing critical financial or personal information to unauthorized entities.

2.8 Emerging Cyber Crimes[1,2,3]

Various attacks reported in the literature are Data Theft, Unauthorized Access, Email abuse, Data alteration, DoS attacks , virus attacks and the like. Some of the **Emerging Cyber Crimes/** attacks are illustrated as below:

Data Theft /Intellectual Property (IPR **)Theft:** Due to the importance of data, the piracy of Data, is a threat, faced by the I.T. players. IPR crimes allows access to patent, trade secrets, copy rights, domain name and data thefts deals with customer data, sales trends, credit card information and any confidential information. The statistics reveals 33% of cybercrime is data stealing.

Email abuse: Email abuse takes many forms like unsolicited commercial email, unsolicited bulk email, mail bombs, email harassment, email containing abusive or offensive content.

Unauthorized access: The person without permission from the owner, connect to or use a system, gains entry in a manner unintended by the system owner and view the private accounts, confidential information, messages, files or resources.

Data Alteration: By changing /modifying / deleting data causes major losses in the Cyber world. A crime reported in USA (Cyber murder), a patient file data altered by a criminal cause overdose of medicine and patient get killed.

Damage of company service networks: This can occur if someone plants a Trojan horse, conducts a denial of service attack, installs an unauthorized modem, or installs a back door to allow others to gain access to the network or system.

Financial fraud: This pertains to anything that uses fraudulent solicitation to prospective victims to conduct fraudulent transactions.

Hacker system penetrations: These occur via the use of sniffers, rootkits, and other tools that take advantage of vulnerabilities of systems or software.

Distribution and execution of viruses and worms: Viruses, worms and Trojans are the types of malicious code which enters into the system without permission of the user and deletes, modifies and captures the user files and data.

Child pornography: refers to images or and in some cases writings depicting sexually explicit activities involving as such, child pornography is a record of child sexual abuse.

Cyber-Terrorism: is unlawful attacks and threats of attack via electronic communications against computers, networks and storage information to control destructive action on public utilities , critical government infrastructure and disruption of communications between governments to intimidate or coerce a government or its people for propagating hidden political or unlawful social and religious agendas.

Cryptojacking: According to the internet security company Kaspersky, cryptojacking is an act of hacking or gaining unauthorised access by infecting a website or manipulating the victim to click on a malicious link or use online ads with crypto mining JavaScript code into someone else's computer, smartphone, and other electronic devices and using its resources for mining cryptocurrency(bitcoin) and other Proof-of-Work cryptocurrencies using the host's resources without the host noticing it or it is too late to know about the attack. Cryptojacking is a cyber attack wherein a computing device is hijacked and controlled by the attacker, and its resources are used to illicitly mine cryptocurrency.

Watering Hole Attack refers to hackers stalking computer users of targeted organizations on the internet for accessing the web sites. Computer user is a particular group of an organization, region or even an entire sector, such as defence, government or healthcare. Hacker identifies these Websites either by closely monitoring the group or by guessing or social engineering. Hackers infect these websites with malware, which infects the victims' systems or compromised web site is used to enable the distribution of malware. The malware in such an attack targets the user's personal information and

to the infected computer.