Study of Privacy Issues During Online Surfing

Swapnil Raj

SOEIT, Sanskriti University, Mathura, Uttar Pradesh, India

Email Id- swapnil.cse@sanskriti.edu.in

ABSTRACT: ***The internet is the quickest method to communicate with others, but it is not the safest. It is full with scams, frauds, and thefts, and everyone who uses the internet is extremely likely to become a victim of one of them. Many people are still ignorant of their internet privacy and are unconcerned about their data being stolen or exposed. These internet users are extremely exposed to cyber-attacks. Many users are spied or conned while using or working on the internet by various persons who want to steal their data or hurt them in some way. As a result, privacy has become a key problem in almost every sector presently. Many hackers and crackers use various methods to steal data all around the world. Malicious software, programmes, data, or code, including as viruses, worms, Trojan horses, and malware, are commonly used to target client servers. This article examines these privacy concerns and how they might be addressed in a variety of ways. It teaches how to prevent falling prey to scammers and becoming entangled in any type of online fraud. The important influence on privacy when we opt to run client server is highlighted in this review study. Everyone has begun using anti-virus software and licenced security products, so there is a lot of room for growth in the future. As scams and fraud instances become more common, the need for these programmes will grow.***

KEYWORDS: ***Internet, Privacy, Security, Server, System.***

INTRODUCTION

The client-server system is a system that functions on both the server and client sides to facilitate data flow between the two. The client-server model's job is to divide the different functions of the client and server amongst them so that all tasks may be completed smoothly. As a result, several users can access the same database at the same time. If a client wants to use a server service, it must first submit a request to the server for that service. The server looks for the service and provides authorization to use it to the client. A client application only runs when it sends a request to the server for a certain service whereas server runs all the time.

While modern technologies have numerous advantages, they also have significant disadvantages. Viruses, Trojans, Worms, and Denial of Service attacks can affect both clients and servers. The mostly used malicious codes are in the form of:

1. *Virus:*

A computer virus is a type of secret code, or a programme, that is created to impact a system in such a manner that when it enters, it modifies the system's functionality and the system is no longer under the control of the user. To function, a virus needs a host. It functions by affixing or injecting itself into a file, document, or programme[1]. The virus remains inert after it has successfully attached itself to the file until the file or document it is attached to is run. When a virus-infected programme or document is launched on a system, the virus begins to work and begins to harm the system by slowing it down, stealing data or passwords, corrupting files, recording keystrokes, spamming your emails and contacts, and even shutting it down. It begins to replicate itself, and it is capable of infecting other systems on the same network.

Emails, messages, Internet file downloads, social media, third-party apps, and a variety of other methods can all be used to propagate a virus. These viruses disguise themselves in such a way that they cannot be detected unless a powerful anti-virus is used[2]. While a virus is still there on system it might produce some symptoms indicating its presence such as:

1.1.Frequent Pop- up windows:

When a virus infects a computer, it may display a series of pop-ups encouraging users to click on various links that might harm the system if they do so.

1.2.Changes Homepage:

The virus may alter the system's homepage, and the user may be unable to restore it, revealing the presence of the infection.

1.3.Sending of Mass emails from the user's account:

The hacker may have gained access to the user's email account and sent emails to other individuals in the user's name.

1.4.Frequent Crashes in System:

A virus may wreak havoc on your hard disc. This might cause the system to freeze or even crash, leaving the user unable to reset or recover.

1.5.System's slow performance:

When a virus infects a computer, it may cause it to run slowly. There is a noticeable change in processing speed.

1.6.Unknown programs start while turning system on:

Unknown applications may be operating on the system. These may show when the system is turned on or may be operating in the background without the user's knowledge.

1.7.Unusual Activities:

Unusual behaviours, such as altering email or system passwords, may occur, preventing the user from successful login.

2. Types of Viruses:
2.1.File-Infecting virus:

These are parasitic viruses that infect data and folders with the extensions.com and.exe. Viruses that bind themselves to executable programmes are known as worms. These can corrupt host files and possibly destroy hard disc formatting[3].

2.2.Micro Virus:

These are most commonly encountered in Microsoft Word or MS Excel documents. These viruses attach themselves to files or documents and propagate when they are transmitted from one machine to another via emails, messages, or pen drives.

2.3.Browser Hijacker:

Browser hijacker infection, as the name implies, modifies browser settings. It alters the browser's route and redirects the user to potentially dangerous websites that the user does not intend to view. It may also modify the browser's home page without the user's awareness and manage a variety of other browser functions[4]

.

2.4.Web Scripting Virus:

It is aimed towards well-known websites. It compromises browser security. Web Scripting Virus attempts to prevent or alter browser operations without the user's authorization. It disseminates through the use of websites. It is incredibly simple to code and disseminate this virus. It is extremely contagious. It modifies the system's browser settings. Cookies are used by these viruses to collect data and to post on social networking sites on behalf of victims using data obtained from cookies.

2.5.Boot Sector Virus:

When a user reboots or restarts their computer, a virus known as the Boot Sector Virus takes control of the machine. An infected USB device placed into the system might transmit the virus. These are mainly found on tangible media like hard discs and USB devices.

2.6.Resident Virus:

These viruses store themselves in the system's memory and utilise that memory to infect the files on the system. Such a virus can cause programme and file corruption by interfering with the operating system.

2.7.Polymorphic Virus:

Anti-virus systems are unable to detect these viruses. When a virus-infected file is run or processed, these viruses change the codes.

Wherever there is a problem, there is also a solution. There is a plethora of reputable anti-virus software available that will prevent any virus from infiltrating the system. These programmes must be updated on a regular basis. These programmes scan, verify, and identify viruses on your computer. These do a rapid and complete scan of the system, identifying and removing all harmful codes, files, and trash applications in order to safeguard the system's security. Precautions should be followed to safeguard the system from being attacked, such as not clicking on random social network links, checking emails before opening any attachments, not clicking on commercial pop-ups, and many other actions that might cause the system to be damaged or insecure.

3. Trojan Horses:

Trojans are malicious programmes designed by cybercriminals to spy on people, steal their personal information, and obtain unauthorised access to their computer or laptop. These take the form of software that appears to be beneficial to users but really contains concealed harmful code that, when executed, grants cyber-criminals access to the machine. Trojan Horses are masters at concealment. Trojans usually mislead users into installing them, then perform their job on the victim's system without informing the victim that anything is going on in their system to achieve their goal. For the concealed virus to work, the victim must execute the file or software that contains it on the system. The system is no longer safe or secure after it has been run[5].

3.1 Types of Trojan Horses:

3.1.1 Backdoor:

Hackers can use this sort of Trojan to get total access to and control of a machine. It allows the user to do whatever they choose to on a computer that has been infected with a virus. They can share data from the infected system to whomever they want, they can receive files of any category and store them in the victim ’s machine, trapping the victim in some misleading or wrong cause, they can launch or install various software into the system, they can remove important documents from the system, and they can even reboot or reset the entire system, causing the victim to lose all of his data. These backdoors may be used to create a network of many virus-infected machines, allowing the spier to manage the entire network. This type of network is known as a botnet, and it can be used to infect and attack many other computers for unlawful and criminal purposes[6].

3.1.2 Rootkit:

These are Trojans which are designed to hide few activities in the system. Main objective of these programs is to prevent all the malicious programs from being detected in a system so that the spier gets the time to do the maximum damage to the victim’s system through virus infected programs by running them as much as he can.

3.1.3 Banker:

These are programmes that are meant to steal information from accounts associated with internet banking, credit cards, e-payment systems, and debit cards. This sort of Trojan horse primarily targets data or files that include the user's personal information and are used to conduct all online transactions.

3.1.4 Exploit:

These are applications that are designed to target a certain application or piece of software that is already installed on the system. These Trojans attempt to inject a code into the system using software that may already be insecure, and then exploit it.

3.1.5 Clampi:

Ligats and Ilomo are two terms for Trojans of this type. The majority of the time, this malware targets banking and financial data or information. It aims to acquire online banking information or login credentials for a shopping site so that when the user buys something and pays for it online, the spier can take the credit card or debit card information, which the criminal can exploit for his own gain. The Clampi Trojan is clever enough to evade being detected by firewalls for lengthy periods of time.

3.1.6 Cryxos:

This Trojan is linked to fraudulent support calls, false messages, and fake OTPs (One time password). When this Trojan infects a system, victims typically receive a pop-up message that contains frightening messages such as "Device hacked" or similar messages that scare the user into seeking help, which is where their phone number, which is attached to the message to contact for customer support, comes into play. Victims frequently fall into the trap and call the number thinking they are calling actual customer service for assistance, only to be directed to the spier's number, which then demands a large sum of money to fix the system and, in some cases, pressures them to give access to their system, resulting in system hijacking and data theft.

3.1.7 Distributed Denial of Service (DDoS) Trojans:

Distributed Denial of Service (DDoS) is a type of distributed denial Trojans are usually directed towards a specific web site. To carry out this process, the criminal infects numerous computers with the virus and then sends repeated requests to the target address via his own system and all of these systems. The target address typically does not have enough resources to process all of these incoming requests, causing the system to enter the denial-of-service zone, where the machine is disabled due to not being able to manage huge number of requests.

3.1.8 Geost Trojan:

Trojans that hide in apps obtained from unauthorised sources are known as Geost Trojans. When the programme in which it is concealed is downloaded and installed, it requests a number of rights, including storage access, location access, media access, and a few more. When the user grants any of these rights, the Trojan begins to operate, infecting the machine and causing it to malfunction. These Trojans steal sensitive information like as banking information, which leads to money theft, putting the victim in a far worse predicament.

3.1.9 IM (Instant message) Trojan:

Instant Message programmes are Trojans that steal user data, including logins and passwords, for a variety of messaging apps, including Snapchat, Instagram, WhatsApp, Telegram, Facebook Messenger, Skype, and others. Criminals can use these Trojans to take control of the chat box, chat sessions, and transfer infected files to other individuals in the victim's address book via the victim's message box. The hacker is able to propagate his malicious code and attack and control several computers this way. They can even utilise the user's machine to launch DDoS assaults.

3.1.10 Wacatac Trojan:

It is an extremely dangerous Trojan that causes significant damage to the target system. It has the ability to carry out a variety of harmful operations on the target machine. It generally infects the target machine via phishing emails, occasionally during the file sharing procedure between systems if one is already infected, and in the form of software patches. Its major goal is to collect personal and private information, then share that information with hackers so that they may exploit it. Hackers can use this to get remote access to the system and do a variety of malicious actions.

4. Worms:

Worms, unlike viruses, do not require attachment to any host, file, or document. A worm can replicate itself indefinitely without the need for human intervention. It does not require any software to harm the system. Worms can be spread through software flaws or as file attachments in spam emails or instant chats (IMs)[7]. When these files are opened, they may give links to dangerous websites or download the worm automatically.

Once within the system, these worms begin infecting files without the user's awareness. They change and destroy the files on the system. They may even implant more malicious software onto the system at times. A computer worm's primary goal is often to simply produce copies of itself over and over again, resulting in the exhaustion of system resources such as bandwidth or hard drive space via overloading a shared network. Worms almost seldom target files on a single machine. Instead, they target and hijack whole networks in an attempt to build a massive botnet network[8].

5. *Search Engines:*

Search engines are software that is used to search the internet for various data or information. These search engines keep note of what the user searches for as well as the websites that the user visits. Furthermore, if the search engine provider also manufactures a browser like Google Chrome, Firefox, or Internet Explorer, they have access to all of the user's browsing history, including any sites he visited or anything entered into the search box. The user's search history, cookies, IP addresses, and click-through history are all collected by search engines. As a result, if a cyber-criminal is spying on someone's search engines, a lot of personal information might be compromised.

6. *Cookies/Online Tracking:*

Cookies are generally considered to be harmless. However, when a third-party application is engaged, they become a source of concern. When a user visits a website, the browser collects all of the relevant data and information from a variety of sources to determine which adverts the user will see. Tracking cookies are used to collect information about a user without their consent. These pose a serious risk to internet privacy. All of this data may be used to construct browser history profiles, allowing advertisers to target users with relevant ads[9].

There is a variety of security software available that protects the system against harmful codes and viruses. Viruses, worms, and Trojans are all prevented by this programme. Various types of safety software are available.

7. *Firewall:*

A firewall is a network security device that protects the system from viruses, worms, and other malicious software. Firewalls monitor and filter all incoming and outgoing data traffic depending on an organization's already defined security rules. A firewall may be thought of as a system's bodyguard. It's a firewall that separates a private internal network from the public Internet. The main goal of a firewall is to keep all potentially harmful material out while allowing non-threatening traffic to pass freely[10].

Firewalls are designed to find and stop any malware or application-layer assaults that may be present in the system. The detection and response times of Next Generation Firewalls are extremely rapid. They have a proclivity for detecting external assaults throughout the whole network extremely rapidly. Firewalls create policies to protect the user's network to the best of its ability, doing fast scans and taking action to identify any invasive or suspicious behaviour, such as malware, and shutting down the system if any such suspicion is discovered to avoid further harm.

DISCUSSION

With the growing number of users, the worldwide network is becoming into not just a source of news, but also a repository for a vast quantity of sensitive data. Nowadays, such data is gathered, processed, and analysed without the agreement of the user. This allows thieves to easily leak and steal personal data with the intent of causing harm to the user. According to the report, there are several ways for someone to get access to a system without the user's awareness, make modifications to the system, destroy and steal data, and even seize control of the system. There are strategies and techniques that may be used to avoid becoming subject to assaults and traps like worms, viruses, and Trojans. People who are surfing the web should avoid clicking on random links and pop-ups that appear while they are working. Before opening any attachments attached to an email, it's a good idea to scan it first. Third-party apps from less reputable websites should be avoided. Emails from unknown sources should be ignored and banned. There is also software that may be used to safeguard a computer system from such thefts and actions. There is both free and commercial software available that ensures the system's security. System safety may be assured by employing these diverse techniques.

CONCLUSION

Online privacy, also known as internet privacy or digital privacy, relates to how much personal data, browsing history, or financial information about a person is kept secret while surfing the internet. People are increasingly concerned about the possibility of their personal data, such as browser history and other information, being leaked or stolen when they are online. We are all sophisticated enough to see and remember that nothing is free, whether it is a downloadable programme, a company's free email service, or a social networking site like Facebook or Messenger Even when a person visits a website, the data about that person is shared with the site they are viewing.

The number of individuals who use the internet and rely on it is growing every day, and many of them are unaware that personal information about them is being gathered. Many people, on the other hand, who are worried about their privacy, limit their internet usage to avoid their data being stolen or leaked through numerous sites. There are a variety of safety steps and safeguards that should be followed to ensure that you are not exposed to dangerous codes, software, or malware. Anti-virus software should be used to protect personal information.

The author has discussed why it is critical to keep data safe and secure, as well as what procedures and precautions can be done to avoid being a victim of scams and frauds. Scammers and criminals may and do steal data from internet users using a variety of cookies, tracking engines, and other ways, as detailed by the author. The author also discusses how anti-virus software may be used to avoid these attacks. Everyone has begun using anti-virus software and licenced security products, so there is a lot of room for growth in the future. As scams and fraud instances become more common, the need for these programmes will grow.

REFERENCES

[1] S. Bahukhandi and S. S. Rana, “Introduction & History of Computer Viruses,” *Int. J. Sci. Eng. Res.*, 2016.

[2] F. Cohen, “Computer viruses. Theory and experiments,” *Comput. Secur.*, vol. 6, no. 1, 1987, doi: 10.1016/0167-4048(87)90122-2.

[3] I. Khan, “An introduction to computer viruses: Problems and solutions,” *Libr. Hi Tech News*, vol. 29, no. 7, 2012, doi: 10.1108/07419051211280036.

[4] R. R. Moeller, “Computer viruses,” *Inf. Syst. Secur.*, 1992, doi: 10.1080/19393559208551314.

[5] Z. Zhenfang, “Study on Computer Trojan Horse Virus and Its Prevention,” *Int. J. Eng. Appl. Sci.*, vol. 2, no. 8, 2015.

[6] F. Chaudhari and S. Patel, “A Survey: Trojan horse Detection Techniques in Network,” *Int. J. Comput. Math. Sci. IJCMS ISSN*, vol. 6, 2017.

[7] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, “A taxonomy of computer worms,” 2003, doi: 10.1145/948187.948190.

[8] F. B. Cohen, “A formal definition of computer worms and some related results,” *Comput. Secur.*, 1992, doi: 10.1016/0167-4048(92)90144-G.

[9] A. D. Miyazaki, “Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage,” *J. Public Policy Mark.*, vol. 27, no. 1, 2008, doi: 10.1509/jppm.27.1.19.

[10] S. G. Pundkar and G. R. Bamnote, “Analysis of Firewall Technology in Computer Network Security,” *Int. J. Comput. Sci. Mob. Comput.*, 2014.