POTC model for Safe and Secure Cyber Communication as well as Transactions

Desai Ami Shaileshkumar[1]
PhD Scholar of R.K.University, Rajkot
amijvaidya@gmail.com

Dr. Sanjay Buch[2]
Asst. Vice President Of Reliance Industries Ltd
(PhD Guide)

Abstract: We are currently living in an age, where the use of the Internet has become second nature to millions of people. Not only business but all types of organization is depend on the Internet. More and more home users are practice the huge benefit of the Internet.

However, this dependency and use of the Internet bring new and dangerous risks. This is due to increasing attempts from unauthorised third parties to compromise private information for their own benefit – the whole wide area of cyber crime. Cyber crime is also increase in cases of unawareness about online fraud and risks. Therefore it is essential that all users understand the risks of using Internet, the importance of securing their personal information and the consequences if it is not used properly. Hackers target home users due to this vulnerability. Due to improper development of website security and loopholes hackers can easily take benefit.

This paper specify current frauds and proposes a POTC model, which provide guideline to home users as well as developer. POTC model proposes a way to improve information security awareness among home users and developer by presenting some information security steps.

Keyword: *Information security, Information security awareness, home user, Hacking, Spam, Malware, Web services, stakeholders, victim*

ABBREVIATION

SOA- Service Oriented Architecture
WPA2-Wi-Fi Protected Access II
TFA - Two-Factor Authentication
VPN - Virtual Privet Network
SSL – Secured Service Layer
CDN - Content Delivery Network
ICMP - Internet control Message Protocol
POTC – Protection of Online Transaction and Communication

*****

I. INTRODUCTION

Now a days many people are attached with each other using web technology. Many service providers deliver facilities to exchange of ideas, information, videos, pictures, and graphics based on SOA. It also allows easy sharing and distribution of existing content to others, due to that professional work can be shared through on-line networks [9].

Using Social networking websites maximum people share or transfer images, video clips, text and personal details without any precautions and bothering about fraud. On-line transactions are done without any security check because many of them do not have awareness about on-line fraud and cyber crime. Thus, hackers can easily hack and misuse their information. The issues include privacy issues, identity theft[5], social networks spam, social networks malware, and physical threats.[8] There are certain issues regarding on-line fraud are describe as below,

- **Hacking:** This is a type of common crime, in which a person's computer is becoming out of order so that his/her personal and sensitive information as well as the entire device can be accessed by unauthorized person's. In hacking the criminal, uses variety of different software's to enter into a person's computer unknowingly without his awareness. [6][13]
- **Theft:** This crime occurs when person violence copyrights laws by downloading music, movies, games and software. Generally, license version software is costly hence culprit person can crack its license software and use for profit. To use cracked software, company's logo, domain name and idea of good name websites for misguide people is also consider as crime.[6][5]

- **Cyber Stalking:** This is a kind of online harassment wherein the victim is subjected to a bombardment of online messages and emails.[4] Typically, these stalkers know their victims and instead of alternative to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more depressed.[6]
- **Identity Theft:** This has become a major problem when people use the Internet for money transactions and online banking services.[10] In this cyber crime, a criminal accesses data of a person like bank account, credit & debit cards details, Social security and other sensitive information to draw off money or to buy things online on the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history also. [3][7]
- **Malicious Software:** These are Internet-based software's or programs which are used to disturb the entire network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system. While surfing such websites these malicious software pop up and ask to download, as soon as downloading starts they start damaging victim's network and system.
- **Child soliciting and Abuse:** In this type of cyber crime wherein criminals solicit minors through chat rooms for the purpose of child pornography. Many Investigating companies or agencies has been spending a lot of time to monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.
- In general, most of the website developers are testing their websites using white box testing, black box testing and gray box testing for protection.[1] After web hosting, some web automated tools are provided in SOA for performance, load and security testing like Soap, Apache jmeter, Curl, Jconsole, Jprofiler, Jira, Bugzilla, Mantic, Redmine, SET, SSL etc. [14]

Current scenario of data transfer in web applications

Data will be exchanged between source to destination using different network and IP address which maybe varying. Because when router is switched off, public IP address of that router will be changed. Sometimes, range of IP address are allocate for a DNS (i.e www.google.com has IP address range like 64.233.160.0 - 64.233.191.255). Communication of data is shown in given figure as bellow:

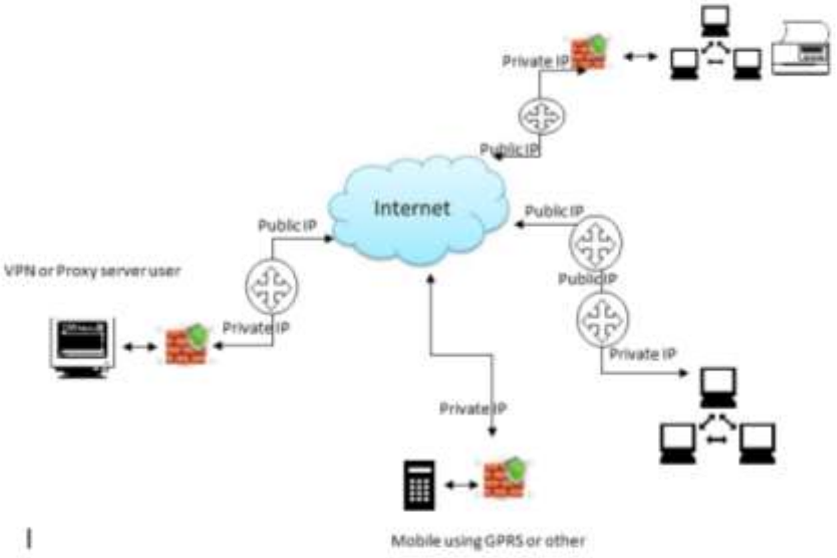


Figure1. Data transfer over network

In this communication, data will be generally transferred through HTTP/HTTPS protocols. Even if data is transferred using HTTPS which is secure connection, still hacking is possible because it also depends on OS, open ports, Security software, User's Password, ISP and Routers etc.

Provision of 100% protection from all aspects of different attacks is not possible. There are some techniques available which makes it possible as well as difficult to hack by any random fly-by hacker.

Problems with current scenario
How computer/system/data can be hacked?

1. Using a small script or a program, the hacker can scan any vulnerability loopholes of the victim's system by using tools like acunetix, skyboxsecurity, saintcorporation etc.
2. Open port is a big problem for individual system/device, because if the hacker can find out open ports of the target system easily then the hacker can send backdoors using this open port which may harm victim's system. This can be done easily by a hacker using readymade tools or commands. For example, using Nmap and netstat command of Linux operating system, hacker can get information about IP addresses of victim's system network and open ports of particular IP address.
3. Always check the domain address of a website, which may be redirected automatically to some fake or cloned website while transferring the data. For example, a valid bank transaction maybe redirected to the web page which can function or perform operation without SSL or which maybe a cloned page of a valid bank website.
4. Always avoid website surfing using automatic text suggested in address bar of browser. For example, if a victim types "www.Fa "in address bar of browser, it automatically suggests text as "www.faceb00k.com". If the victim clicks on a suggested text, victim maybe redirected to a dummy DNS. (here "o" is replaced with "0").
5. If the victim gets any unknown hyperlinked text or image via an email or a message on computer or mobile, don't click on that hyperlinked text without verifying that email id or website. To verify details, websites that are already developed are available. For example, (a) victim can verify IP address using "whatsthierip.com" website; (b) victim should check the string at the end of the received email or link, For e.g "*.readnotify.com", if this is the string it redirect's to the Public IP address of hacker's.
6. Victim's at times, use other's system for internet surfing. Victim inserts their personal details, account details, username and passwords which maybe hacked because of the key logger software. Through key logger, data may capture information and store keystroke for hacking purpose.
7. Some websites and readymade tools maybe used for hiding original IP because, it does not maintain log of IP. Cyber ghost, hotspot shield, no-ip, open VPN, ProxyPN etc provide VPN for public IP management and hide original IP of hacker's.
8. Some websites provide facility to generate fake DNS as well as link to collect user's detail which is further used for phishing. Name of Websites are 000webhost.com, 110mb.com, t35.com and hostia.com.
9. Generally Kali Linux is use for penetration testing but it has many developed tools which is used to hack the victim. For example, metaspolit tool is used to hack the victim's device and send viruses, worms and Trojan. It will also take controls of victim's device.
10. Some software is providing dummy port numbers which bind with hacker's public IP address and send the information of victim through tools like NJRate, No-IP, Androrate and Prorate etc. When victim access his/her device, log will be display on hacker's computer. With this log details hacker can easily access victim's device.

Loss of data, during internet transaction is not only the problem of proper technology/testing methods of web server, web services (single/multi stakeholders) or websites, but it is the problems, mistakes, unawareness of client(user's).

II. Methodology and Guidelines

Protection of data is not only the responsibility of developers but it is a composite responsibility of client, website developer and service provider. Following are the course of action to be followed by client.

Protection steps followed by user :
Step 1: Make your passwords strong.
Password is the first line of attack in this digital war between hackers and the potential victims. If hacker can get victims password, the rest is easy. So always use strong passwords. A **strong password** consists of at least six characters (and the more characters, the stronger the **password**) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so

a **strong password** contains letters in both uppercase and lowercase. Example: P455W0RD.

Step 2: Use TFA (Two-Factor Authentication)

Authentication means to identify valid user. To increase systems security two-factor authentication can be used. Which is describes as bellows.

1. Username and password factor
2. Biometrics factor
3. Secret questions factor (which victim have)

Step 3: Refuse click/select unknown and suspicious links.

Do not click on unknown hyperlinked text or images unless verifying the sender email id or website.

Victim can verify unknown sender identification using "whatsthierip.com" tool. For example, If the email address of the sender is followed by "*.readnotify.com" then it redirects victim's Public IP address to hackers. So, Hacker can steal victim's information like passwords, bank account details, brokerage, email accounts, social security number, identity, etc. Information will be sells by hacker in marketing world.

If victim got email from any unknown email id, it will be is trace using following steps,

a. Copy of source content using show original option
b. Paste on header box in ip2location.com->email tracer
c. Then Click lookup button.
d. It will display IP root (source to destination).
e. Check IP root is valid or not.

Step 4: Generally refuse P2P File Sharing Networks

Peer to peer is an unsafe way to transaction. Malware or undetectable backdoor will be attached with music, movies, documents and other files using ready-made tools like NJRATE, PRORATE or ANDROIDRATE etc. When victim downloads the file, backdoor will install automatically in victim's device so, Hacker will get access of victim's system. The solution to this:

a. If victim found any unknown process in the start-up, the path should be accessed from the task manager.
b. Remove the process from msconfig file and delete it from target location.
a. Also delete the file from registry using run->cmd->regedit manually.

Step 5: Update your operating system, software and system regularly.

New security vulnerabilities are discovered daily in operating system and applications. For example operating systems like Windows 7 or 8 and applications like Flash, IE8, and Adobe Reader. Hackers generate exploits for these vulnerabilities to attack.

Soon these "exploits" are passed around to other hackers and everyone is trying to use them against victim. This allows victim to install their software on victim system to control it and steal victim resources and information.

When the software developers such as Adobe, Microsoft, and Apple learn these vulnerabilities, then they develop "patches" to close these loopholes. They offer these patches as updates to the victim, Victim must update to be secure.

Step 6: Use latest and updated Antivirus.

Everyone should have some form of antivirus software on their system. Antivirus software is not perfect, but it is certainly better than nothing.

Even the best Antivirus software is effective to approx. 95% of known malware. i.e. one in 20 pieces of malware will be missed. Some of the lower quality antivirus software will miss 1 in 2 pieces of malware. Antivirus software is only effective if its activated and updated.

Antivirus software can't protect victim from silliness. A well-designed malware can embed itself into the Windows system files and victim's Antivirus software can neither detect nor remove it. In some cases, it can even disable victim's Antivirus software before found out.

Step 7: Do Not Use Adobe Flash

Adobe's Flash Player is available on nearly every computer, tablets, smart phone and even Android devices. It enables us to run those interesting videos as well YouTube, animations, etc. Without it, when victim visits a website with video or animations, he/she gets the warning messages to install Flash Player and a blank screen.

Flash Player is such a poorly designed and coded piece of software that it is known as "hackers best friend".

Step 8: Be secure using good Firewall

Although Microsoft ships a rudimentary firewall with its operating system, it is strongly suggested that victim should install a third-party firewall for better protection and block some request ICMP protocol.

One of the third-party firewall is Zone Alarm's Free Firewall. As the name says, it is free and very effective.

It not only blocks outsiders from getting in, but also stops malware from accessing resources on victim's computer and talking out.

Step 9: Increase security using router setting
Make advance setting for router like WPA/WPA-2, Mac- filtering, block URL, etc. WPA and WPA-2 are two security protocols and security certification programs which provide latest Wi-Fi encryption standard, and the latest encryption protocol. MAC address filtering allows you to define a list of devices and only allow selected devices on your Wi-Fi network. Block URL is provide blocking facility to unwanted websites through utility e.g. tinyproxy, Websense or WFilter.

Step 10: Prevent from social engineering attack
Social engineering attack is very easy and familiar attack. Hackers gathered personal information through offers, phone calls, other person, email, sms or yourself. These collected information are used for identity theft as well as hack organization (in which you belong) by hackers. Thus, never share or disclose your/others personal information via survey call, email, auto reply call etc. Always read terms and condition at the time of open new online account because they may share or resell your information with marketing company or other without any intimation.

Protection steps for web service/website developers:
Step 1: Always hide admin panel because using admin panel hacker can access database and admin site also. Store sensitive information in encrypt format in admin site.

Step 2: User are not allow to insert any script as a user input because many time hacker insert malicious script and backdoor in website/database.
Step 3: Some website like matrimonial, employment, tender etc provide facility to upload files as a user input. Hacker can easily upload backdoor which provide full access to hackers. So validation should be provided to check uploaded file type.

Step 4: If you manage any sensitive information like personal information, account information, etc use SSL or other encryption algorithm to encrypt information.

Step 5: Hackers attack on known keywords and file name like password, admin, username, credit card number, employee no, login.php, user.php, login.aspx, admin.aspx, etc. When you developing a website don't use such known keywords or file name for storing information.

Step 6: At the time of providing facility as a user input, never accept single quote ('), double-dash (--), union, exec, etc. By using such sign or keywords hackers can easily inject sql command and get the information about database. Input constrains to be provided for protection at the time of inserting values.

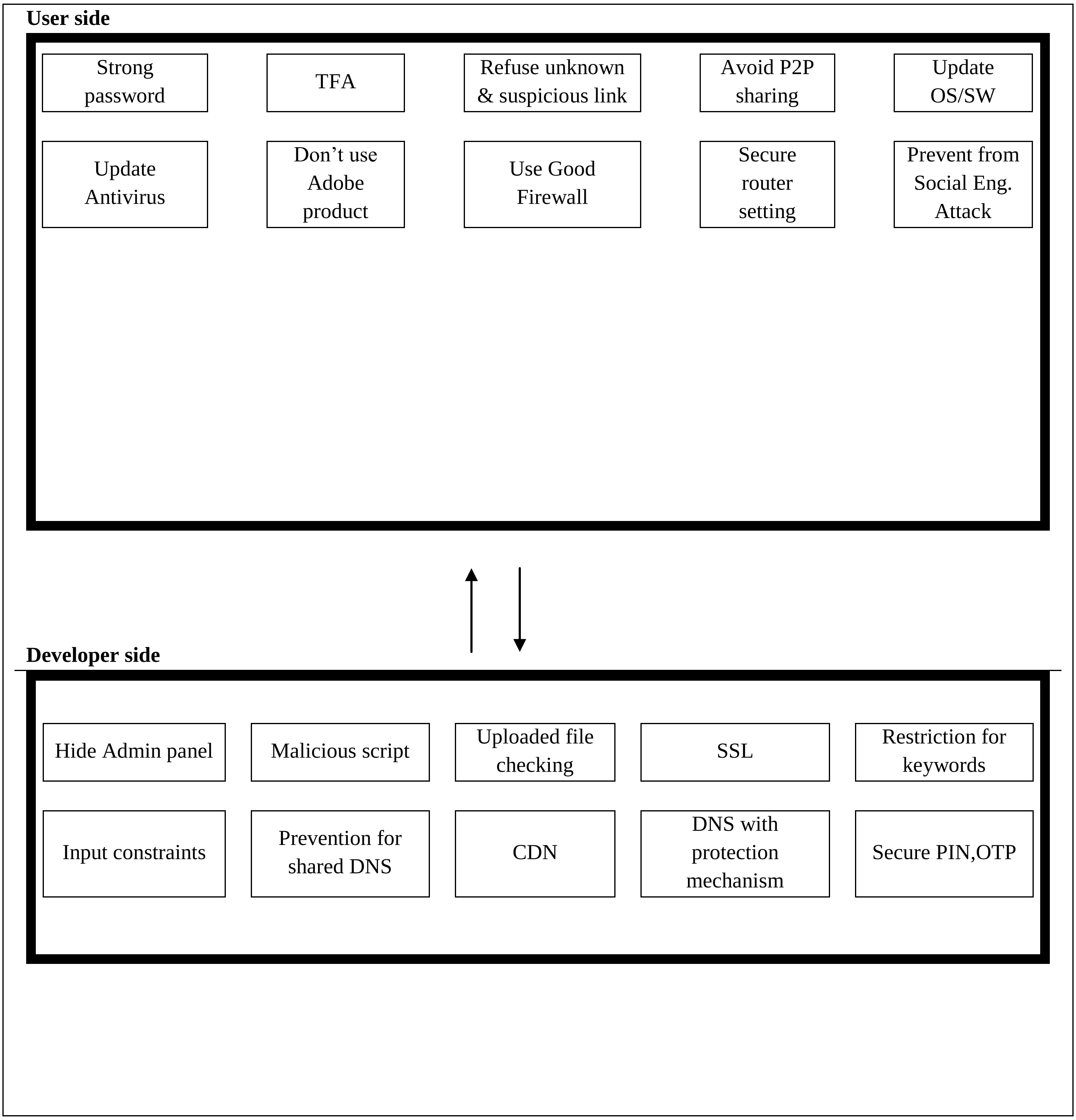
Step 7: Do not publish websites in shared DNS, because if any other website is hacked on shared web server, it can easily get access to victim's website.

Step 8: Purchase domain name with extra protection mechanism which will hide domain name details like providers, IP address, owner details etc.

Step 9: Use CDN (Content Delivery Network) which hides IP address of websites/web services provider.

Step 10: User password, pin number or OTP is generally use for authentication purpose, but it can be trace using brute force attack. Because it is generally between 0 to 999999. For protection purpose generate this type of code in alphanumeric form, so it is difficult to trace or hack.

POTC Model



III. Conclusion

The increasing popularity of online transaction and communication has introduced the needs for additional standards to help support the new security challenges involved in POTC model, but still 100% secure transaction is a big question. In any online communications system, there are some challenges and these challenges are considered as an indicator of the security gaps which generate weakness in the system protection and are vulnerable to attacks. Some online fraud and challenges in web services are mentioned in this paper. Several guidelines for victim and developer has been put forward corresponding with the challenges for secure web transactions. Future work includes extending this approach to develop Security testing/technology/tools for multi stakeholder’s website/web services.

References:

[1] Acharya, Shivani, and Vidhi Pandya. "Bridge between Black Box and White Box – Gray Box Testing

Technique." *International Journal of Electronics and Computer Science Engineering* 2: 175-184.

[2] Adam Kie˙zun, Philip J. Guo,Karthick Jayaraman,Michael D. Ernst. "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks." *Software Engineering, 2009. ICSE 2009. IEEE 31st International Conference* (IEEE), May 2009: 199 - 209.

[3] Ajeet, Singh, Karan Singh, and Shahazad. "A Review: Secure Payment System for Electonic Transaction." *IJARCSSE* 2, no. 3 (march 2012).

[4] Daniel Walnycky a, Ibrahim Baggili a, *, Andrew Marrington b, Jason Moore a,Frank Breitinger. "Network and device forensic analysis of Android social-messaging applications." (ELSEVER) 2015: 577-584.

[5] Goela, Jai Narayan, and BM Mehtreb. "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology." *ICRTC(science direct)* (elsevier) 5 (2015): 710-715.

[6] gunatilaka, Dolvara. *A survey of privacy and security issues in social networks.* http://www.cse.wustly.edu/~jain/cse571-11/ftp/social/index.html.

[7] *Information resellers.* the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, United States: Government office, 2013.

[8] Karumanchi, Sushama, and Anna Squicciarini. "A Large Scale Study of Web Service Vulnerabilities." *Internet Services and Information Security* 5, no. 1 (FEB 2015): 53-69.

[9] Mary-Luz Sánchez-Gordóna, Lourdes Morenoa. "Toward an integration of Web accessibility into testing processes." Edited by Procedia Computer Science 27. *5th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion, DSAI 2013.* ELSESIVER, 2014. 281 – 291.

[10] Normalini, M.K., T. Ramayah. "Biometrics Technologies Implementation in Internet Banking Reduce Security Issues?" *International Congress on Interdisciplinary Business and Social Science* (ELSEVER), 2012: 365-369.

[11] Patil, sheetal, and S D Joshi. "Identification of Performance Improving Factors for Web Application by Performance Testing." *IJETAE* 2, no. 8 (Aug 2012): 433-436.

[12] Pressman, Roger S. *Software Engineering.* Vol. 1. New york: McGraw-Hill, 2001.

[13] Tan Phan, Jun Han, Garth Heward,Steve Versteeg. "Protecting Data in Multi-Stakeholder Web Service." no. 978-1-60558-799. ACM, april 2010.

[14] Yunus, Mamoon. "Fundamentals of SOA Security Testing." *Service Technology Magazine*, Feb 2012: 1-6.