A Detailed Survey and Classification of Commonly Recurring Cyber Attacks

Jaideep Singh
Computer Science Department
CKDIMT Amritsar

Simarpreet Kaur
Computer Science Department
CKDIMT Amritsar

Gurminder Kaur
Computer Science Department
CKDIMT Amritsar

Goldendeep Kaur
CSE Department
GNE Ludhiana

ABSTRACT
Although the computing devices in today's era can be compromised in a variety of ways, this research paper delves deep into different types of cyber attacks that strip out security from the innocent clients. The impact of these attacks depend more on the broad spectrum of opportunities that a novice user serves to an attacker unknowingly. Though a client sometimes has minimum power to withstand the technical prowess of a skilled attacker, still the probability of such attacks can be nullified by reducing the vulnerabilities of a particular computing system. Thus conscious risk management strategies need to be implemented to save organizations and billions of users across the world surfing the web wirelessly. The paper starts with a brief introduction about various wireless attacks that are frequently carried out in a local area network and their classifications. The research presents several schemes for detecting, mitigating and preventing such type of precarious attacks. Role of user awareness in diminishing the threatening effects of such assaults has been specially taken into consideration. The important features and limitations of the already reported methods against protection of such attacks have been examined**.**

Keywords
Cyber Assaults, User Awareness, Risk Management, Local Area Networks .

1. INTRODUCTION
In the modern era of information technology and computing the cyber attacks are increasing at an alarming rate. Most of the organizations in the world are being compromised for information in one way or the other. It may be through some harmful attack using web**,** or through malicious code downloads (direct or indirect). Cyber attack is an attempt by hackers to destroy, disrupt or damage a computer network using social engineering techniques. Cyber criminals have learned several techniques to hamper the working of a computer systems mostly used in banking, business etc. Mobile worms, Malware, phishing, DoS and DDoS are the principal methods of assaults that are teasing the cyber agencies for so new solutions every now and then. These attacks can be carried out through social sites or using Software engineering techniques. With the growth of social media in India**,** the number of cyber attacks have also increased proportionally. [19] As a result, India ranks second in the number of cyber attack victims in 2014.

Currently, Cyber Crime is considered as a great hurdle to the economical and technological growth as per the recent researches. As a result of major and fast developments in the technological fields, the level of living has improved. These threats are called Cyber Attacks. Circulating wrong information, cripple services, accessing secret information in an unauthorized way and espionage etc. all can be done by disrupting a computer system. [2]As an approach to cyber security, each and every organization should implement security measures to the level that they cannot be breached. If they are still breached, then it means that they still possess some vulnerability (soft points)**.**[9] As a result of these vulnerabilities, an attacker can pretty easily exploit a system, regardless of what types of tools are being used or what genre of attack it is. Due to the lack of awareness in users about cyber attacks and their types, the organization's networks are left with vulnerabilities. These vulnerabilities serve as a path for hackers to steal or spy useful information regarding records or financial transactions etc. using spy ware or Trojan horses. As a result, the complexity and severity of these attacks has been increasing day by day. By knowing the motivation or aim behind an attack, the programmers can create a security program or surveillance mechanisms.

Cyber attackers, first scan the web, and then choose or focus those systems that are left with vulnerabilities or weak security mechanisms. Cyber attacks are not carried out just for organizations or institutes, but in between nations or countries also. A country would want to penetrate into the official information of other countries, with the help of malicious tools and this has become a common phenomenon these days. "India as a country is most vulnerable to cyber security attacks. This gets more complicated given that the authorities in the government and private sector are not geared up to tackle the menace as a comprehensive strategy".[14]

This paper emphasizes upon the various types of cyber assaults and various risk management strategies that are currently being used to prevent such attacks. Furthermore the role of user Awareness in pacifying such attacks has also been taken into account,.

2. CLASSIFICATION OF CYBER ATTACKS

2.1 Denial of service (Dos)
These types of attacks are initiated by a complete group of attackers or simply an individual, with the aim of disturbing Internet protocols (IPs Packets) to stop users to effectively access the internet. There's not a single way to attack a computer network, but are many. [1]

Denial of service attacks are classified in following three major types:-

I: Resource Degradation: These are the attacks, due to which the target (the resource or device) stops working simultaneously and effectively.

II: Networks Deluge: Attacks that attempt to submerge the bandwidth tolerance of network device such as Routers, Modems etc.

III: Scathing: Destroying or Disturbing the ability of a device, to perform operations accurately and effectively, such as power interruptions etc. are termed as destructive or scathing attacks.

On the whole, the aim of an attacker is basically to disrupt a computer network or smash a computer system by making interferences with the information, to deny the service to the users, for proper development of economy, prevention from these attacks is very important as they can harm various sectors of a state or country. Developing security features against DoS attacks is of prime importance in the modern state of art. [2]

2.2 Man in the middle attack (MitM)

The tools or mechanisms used to steal information by working against some specific protocols, from databases, e-mails etc without the knowledge of the one who is using it, is termed as an **Access Attack.[**1] This can easily be elaborated using the example of **Eavesdropping**.

In Eavesdropping, a person can listen to or read the information between communicators, without their consent. In this, the attacker makes the communicators think that they are directly talking to each other, but in actual, the attacker can read the relevant information and can even change the content, inject new messages or malicious codes into the conversation. So, the attack in which an attacker intrudes into the communication of parties, and is able to modify or add data into the conversation is called a Man in the Middle attack. Many of OS X's most popular apps were recently revealed to be Vulnerable to man-in-the-middle (MiTM) attacks. [13][20] This is also known as Janus attack or Bucket Brigade Attack or Session Hijacking Attack (SHA), and is a form of eavesdropping. Though there are various types of MitM attacks based on different scenarios but here discussed are the most recurring MitM attack that is ARP Poisoning.

ARP Poisoning: This refers to poisoning of Address resolution Protocol (ARP). All the devices used for internet access have a Network Interface card which has an unique address called the MAC address (Media Access control address.)In a Local Area Network (LAN), the attached devices have their address as long as 48 bits.ARP is used to map MAC address to IP (Internet Protocol) address, where an ARP table is used to maintain a link between each MAC and its corresponding IP Address.ARP provides address conversation in both directions and protocol rules for maintaining this correlation.[17][9]

In ARP Poisoning, the hacker would fit his computer or device in between the communicators, so as to steal the information or to be in the path of two target computers for injecting malicious codes or acquiring information without the permission of those two. During this procedure, the attacker would keep forwarding the frames to them so as to not disrupt the communication. So, the attack is performed as follows:

C1 and C2 are two targets.

A is the attacker.

- **(i)** A poisons the cache of C1 and C2.
- **(ii)** C1 associates C2's IP with A's MAC.
- **(iii)** C2 associates C1's IP with A's MAC.
- **(iv)** All of C1 and C2's traffic(information) will then go to A first, before going to the destination i.e. the messages would not be directly sent or received.

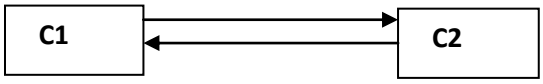


Figure1: Right flow of Packets

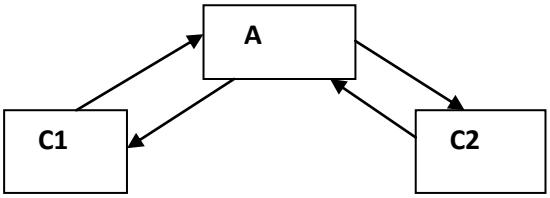


Figure2: Redirected flow of Packet

2.3 Brute force

The use of internet has made computer users to generate passwords so as to open an e-mail account, use e-banking, retrieving an e-mail etc. Passwords, also known as watchwords are being used for a long time and are always kept private from the users who are not allowed to use that particular system or service. For the recovery of a forgotten password or to get an unauthorized access to a system, there's a technique of guessing, cracking or attempting to hack passwords, which is known as Password cracking. A user keeps guessing the password until the password found is correct.[18] Although, there are different methods to hack a password.Some of the major ways to achieve cracking are listed below:

I:Dictionaries: Mostly, watchwords are a combination of simple English words. So, to crack a password, a file of dictionaries is passed through a user's account or database. If any of the words is matched with the password, then the user hacking the password gets an access to the specific system or service. This is called Dictionary attack.[3]

II: Hybrid: Adding numbers or symbols to passwords is a simple way used by users to add security the passwords. A hybrid attack acts as same as like dictionary attack with just one difference, that it adds special symbols or numbers in the passwords to gain access to the system. [16]

III: Brute force: It is the most time consuming way to crack a password. In brute Force, each and every combination of letters and numbers is tried until the password is cracked.

Like other attacks, it can also be divided into sub-categories. Brute force is mainly of two types- targeted and untargeted (Trawling Attack).[3]

Targeted Brute Force: In a targeted attack, various combinations of alphabets and numbers are tried so as to crack the password of the account, the attack is targeted at. If the password is successfully cracked, then the attacker successfully gets unauthorized access to the account. [6]

Untargeted Brute Force: The attack where a particular password is chosen instead of an account, and that password is tried on every account in scope.

2.4 Backdoor Injection

When a user surfing the internet enters some database to search for, before the results display, various steps are performed at the backend. Suppose a user needs to search for a book online. After, entering the name of the book, the input is sent to the server of the website on which the search has been made. Now the server has to have something to read the given input, so as to give the desired results. Here, the source code of the application works. The source code converts the form of input into SQL query. This SQL is then sent to the database, where there is an organized form of data present. The database reads the query and shows results. SQL is "structured query language" that is used to create databases. Some examples of SQL are MySQL, Oracle etc. Ransom ware hackers trick victims into visiting an infected Web site or downloading an attachment and then encrypt their data. Hackers post a ransom note on a user's screen; if the victim does not pay within a certain amount of time, their data is lost forever.[15] In backdoor Injection attack, the attacker tries to modify the output. But, the application source code and the database is not directly accessible. So the attacker needs to have control over the input of the user, so as to change the outputs successfully. Thus, it is safe to conclude that the attacker will try to change the input so as to change the output, by using the SQL Injection attack (SQLIA) technique.[4]

A database is an organized collection of data that can be public or confidential, which may relate to the Banking services, Finance, Defense etc. an attacker with the intention to access data fro the database in an unauthorized manner, or to steal confidential information from it, can use SQL Injection (SQLI)as a technique to attain the goal. The attacker inserts or injects wrong SQL query to the application.
As some applications have access to database, the altered SQL query can ten read secret data from database, make changes in it like creating/ deleting /editing/ upgrading and perform administrative operations like recovering a file or shutting down the database and much more.[5]
The vulnerability of websites to these attacks has been increasing year by yea. This is the reason why SQL injection has been termed as one of the most dangerous attacks. Large Botnets are used by the attackers to find out the vulnerable websites i.e. the websites on which attackers can inject malicious SQL query.

Based on recent surveys and researches, the four principal attacks in cyber security were shortlisted and a review of these techniques was provided in Section-2.

Section-3 provides the existing methods used to detect these cyber attacks, Section 4 provides the Comparative Analysis of these attacks keeping in view the vulnerability level of such attacks and Section 5 includes the open issues and future scope.

3. LITERATURE REVIEW

These cyber attacks on the network can go completely undetected if appropriate measures are not taken. It has been observed that there is no universal defense against these attacks. Various methods are used to detect the different types of attacks. One of the simplest methods to prevent man in the middle attacks is to use static ARP entries. As static entries cannot be updated, spoofed ARP replies can be ignored. But this method is not suitable practically for large networks to manually add each entry into the cache. Free Intrusion Detection Systems like Snort , ARPWatch , XArp are working on detection mechanism but not able to provide complete defence. Kernel based patches like Anticap and Antidote prevents ARP poisoning by rejecting the ARP replies that contains a MAC address different from the current entry in the cache for same IP address. But this solution is also available for a limited number of specific kernels. On the other hand, Port Security detects MAC cloning but does not able to prevent ARP Spoofing. Some High end Cisco switches proposed a feature known as Dynamic ARP Inspection that allows the switch to block invalid <IP, MAC> pairings. It uses local pairing table that is built using a feature known as DHCP snooping to detect which pairings are invalid. But the high cost of switches makes this feature ineffective.

Common measures of TCP SYN Flood attack defence have host-based and firewall-based two types. Previously, ways of TCP SYN Flood attack defence include increasing the size of Backlog, shorten the TCP connect overtime and SYN Cookies etc. Recently Chen[20]proposed methods based on identifying IP-spoofing. Sun[21]suggested ways based on bloom filter combined with Change Point Detection Technology. However, methods mentioned above cannot effectively defense large scale of TCP SYN Flood attacks or SYN Flood plus Ack Flood attacks.

WIDZ[22], a tool used to defend wireless network proposed by FatBLOKE is only a proof on concept - It is not up to great software packages like Snort etc that you might find on sourceforge. WIDZ project contains a number of very simple programs. They are designed to cover three of the major 802.11 risks: Unauthorized Aps, War Driving, Flooding (Picks up attempts to flood the AP with associations). It is a "proof of concept" as such is not intend to be run, except under lab conditions that you deem adequate and secure. Its development has been bogged down by a series of trials some technical, some managerial.

4. COMPARATIVE ANALYSIS

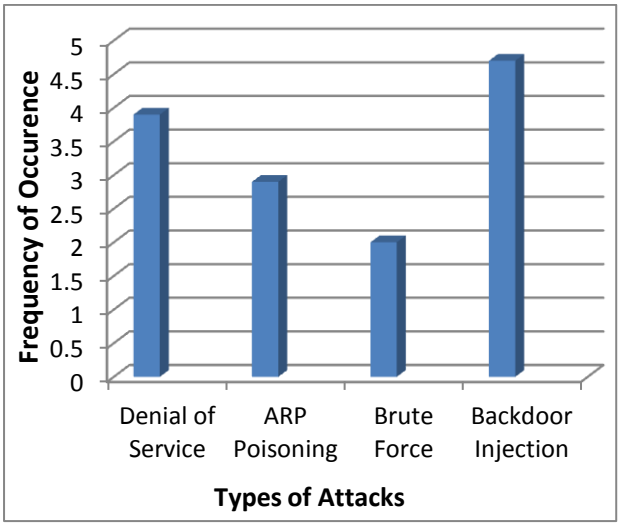
Based on the severity of threat posed by various cyber attacks towards the information exchanged over computer networks today, Table 1.1 depicts the analysis.

Table1

S. no.	Attack	Operation	Vulnerability Level	Frequency of Occurrence
1.	Denial of Service(DoS)	Dos attack stops the services of a Computer network by using Botnets to flood packets.	High	High
2.	ARP Poisoning(MitM)	This attack is used to successfully get unapproved access to the information flowing between users and even changing or disrupting the	High to Medium	Very high

		messages		
3.	Brute Force	Passwords are cracked by trying various expected passwords, for getting access to an access point.	Low	Moderate
4.	Backdoor injection	It is used to change the output of an entered input (query), by making changes with the entered query.	Very High	High

Concluding from the comparative analysis, the following bar chart depicts the frequency of occurrence of varied cyber assaults.



Observing from the tabular analysis and descriptive bar graph , it may thus be inference that backdoor injection is the most frequent attack. Also Vulnerability level is the highest among all the exploits followed by ARP Poisoning, Denial of Service and Brute force.

5. OPEN ISSUES AND FUTURE SCOPE

After delving deep into the literature and researches conducted by learned academicians in cyber security domain, it has been brought out that there are still no ideal preventive solutions to the principal cyber assaults .After this endeavor, future research will try to identify best solutions that have been devised as yet to plug these attacks worldwide. Furthermore the research can be extended by collecting data of graduate students based on their awareness towards the principal attacks.

6. REFERENCES

[1] M. Uma and G. Padmavathi, "*A Survey on Various Cyber Attacks and Their Classification*", in the proceedings of International Journal of Network Security, Vol. 15, p.p. 390-396 (2013)

[2] Monika Sachdeva, Gurvinder Singh and KrishanKumar, "*Deployment of Distributed Defence against DDoS Attacks in ISP Domain*", in the proceedings of International journal of Computer Applications, Vol. 15,p.p. 25-31(2011)

[3] Carlisle adams and Guy-Vincent Jourdan, "*Lightweight protection against Brute Force Login attacks on Web Applications*", in the proceedings of Privacy Security and Trust (PST), 2010 Eighth Annual International Conference,p.p 181-188 (2010)

[4] Parveen Sadotra "*Hashing technique-SQL injection attack detection and prevention*", in the proceedings of International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3 , p.p 4356-4365 (2015)

[5] Predrag Tasevski, "Password Attacks And Generating Strategies"

[6] Retrievedfrom:http://www.trendmicro.co.in/vinfo/in/security/news/cybercrime-and-digital-threats/using-8-backdoor-techniques-attackers-steal-company-data

[7] Dove Chiu,Shih-Hao Weng,and Joseph Chiu,*"Backdoor use in Trageted Attacks"*

[8] Jaideep Singh and Vinit Grewal, *"A Survey of Different Strategies to Pacify ARP Poisoning Attacks in Wireless Networks"*, in the proceedings of International Journal of Computer Applications, Vol. 116, p.p 25-28 (2015)

[9] C. Barry, L. Lee, and M. Rewers, International Cyber Technology and National Security Policy, National Defense University, June 2009.

[10] M. J. Ranum, *Internet Attacks*, pp.1-37, 1997.

[11] GFI Software, GFI Targeted Cyber Attacks http://www.gfi.com

[12] Retrieved from: http://thenextweb.com/apple/2016/02/09/huge-number-of-mac-apps-are-vulnerable-to-man-in-the-middle-attacks/#gref

[13] Retrieved from:http://www.dqindia.com/india-most-vulnerable-cyber-attacks/

[14] Retrieved from: http://www.scientificamerican.com/article/the-most-vulne rable-ransomware-targets-are-the-institutions-we-rely-on-most/

[15] Retrieved from: http://www.learninghowtohack.com/password-hacking-5-attack-types-hybrid/

[16] Marco Antônio Carnut and João J. C. Gondim, "*ARP spoofing detection on switched ethernet networks: a feasibility study*," 5th Symposium on Security in Informatics held at Brazilian Air Force Technology Institute, November 2003

[17] G. Sowmya and A. Naveen Kumar," Brute force attack – blocking techniques",in the proceedings of international journal of Engineering and Computer

Sciences, Volume2 Issue 8 August, 2013 Page No. 2541-2543.

[18] Retrieved From:https://www.recordedfuture.com/cyber-threat-landscape-basics/

[19] Retrieved from: http://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM

[20] Wei Chen,Dit-Yan Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing", International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, pp. 38, 2006.

[21] Changhua Sun. Jindou Fan and Bin Liu, "A Robust Scheme to Detect SYN Flooding Attacks", Sec. Inter. Conference on Communications and Networking,China , pp. 397-401,2007.

[22] Jaideep Singh, Goldendeep Kaur, Dr. Jyoteesh Malhotra, "A Comprehensive Survey of Current Trends and Challenges to mitigate ARP attacks", In proceedings of 1st International Conference on Electrical, Electronics, Signals and Optimization, ISBN: 978-1-4799-7678-2, 2015 IEEE.

[23] "ARP-Guard," (accessed 28-July-2013). [Online]. Available http://www.arp-guard.com.

[24] Zouheir Trabelsi and Khaled Shuaib. Spoofed ARP Packets Detection in Switched LAN Networks. J. Filipe and M.S. Obaidat (Eds.): ICETE 2013, CCIS 9, pp. 81–91

[25] M. Barnaba, "anticap", (accessed 17 April 2013) Online. Available: http://www.antifork.org/anticap.

[26] V. Goyal and V. Abraham " An efficient Solution to the ARP cache poisoning problem", in Proceedings of 10th Australasian Conference on Information Security and Privacy, Jul 2013, pp 40-51.

[27] I.Teterin, Antidote, SecurityFocus, http://online.securityfocus.com/archive/1/299929, last accessed, Apr. 2012.

[28] M. Gouda and C.-T. Huang. A secure address resolution protocol. *Computer Networks*, 41(1):57–71,Jan.2012