A Literature Review on Sniffing Attacks in Computer Network

Anubhi Kulshrestha*, Sanjay Kumar Dubey**
*Department of CSE, Amity University, Noida, India - 201303
** Department of CSE, Amity University, Noida, India - 201303

ABSTRACT:
In today's modern era, the internet plays very important role among communications of various stakeholders. Internet creates a link between client and server. But the interface between client and server faces various security attacks like content sniffing attack, denial-of-service attack, replay attack, bots, cross site scripting and phishing. Sniffing attack is very difficult to handle. So, this paper focuses on comprehensive review of sniffing attacks, its type, sniffing tools and techniques, online adaptation problem, Scatter net scheme based on sniff mode, sniff project, Wi-Fi sniffing program and other related techniques. Numerous research papers explored for this purpose. Reviewing process also focused on security measures which are applied during the flow of information between client and server. To explore the gap in present area, overcome issues related to sniffing attacks are also discussed in the research paper.

Keywords **-** Attacks, MIME, Phishing, Security, Sniffing, Threats.

I. INTRODUCTION

Every person in this running world trust on web based applications. The world is now-a-days turning digital and the people start storing and sharing their personal data on internet assuming that their information is more secured on internet as compared to the handwritten documents. But they are unaware that the information stored in digital form on web is easily accessible to anyone. To overcome this problem there are three main goals of network security. Confidentiality means only authorized user could access information, or by prevent access or to disclosure of data to unauthorized access. For example- Authentication methods like passwords and identities of user made disclose to unauthorized (wrong person) user [1] .It is related to privacy of information. Integrity refers to trust that the data will remain same and it will not be modified without the knowledge of the authorized user. It also include "source integrity" which means that the information actually belong to the person or the entity in real. Availability includes the availability of information to the authorized user. It may be affected by malfunctioning of computer, human cause (accident), natural phenomenon [1].

II. SNIFFING

Sniffing is a common network security attack in which a program or device takes important information from the network traffic of specific network. The main aim of the sniffer is to steal passwords, files (FTP files, E-mail files), and E-mail text. Various protocols are also prone to sniffing. Sniffing is an attack on confidentiality of data. The basic target of sniffer is to find out the password and other personal information of the user, this compromise the confidentiality. Confidentiality is major challenge for the attackers on the internet. The aim of most of the attackers is to sniff personal details by capturing data which is travelling through air to find the important data. Various types of sniffing are as follows:

2.1 Client Side Sniffing-In this type of sniffing the web page of sniffer uses programming language such as Java script interpreted by user agent sent to web servers. This method is unreliable.

2.2 Server Side Sniffing-This type of sniffing uses communication protocol known as http. Sniffer attacks from server side.

2.3 Browser Sniffing- It is an attack in which websites is used and web applications in order to determine the web. This creates various malicious activities like misinterpretation of HTML, cascading style sheets, etc. Malicious user can easily steal private information of user by sniffing a network. They download free sniffer software from the net and install it in the computer. Sniffer changes their Network Interface Card (NIC) into promiscuous mode, which receives packets and passes it to system kernel. Sniffer displays these packets on hacker's personal computers. Hackers maintain a record by looking at network of users. Sniffing attack is very difficult to detect and also it

is very hard to overcome such types of attacks. Few researchers detect sniffers by two methods like ARP detection and RTT detection [6].

2.4 Content Sniffing: Web based applications reside on server side and worked from client side. These applications suffer various problems as they have vulnerabilities, which leads to stealing of information and generate run time errors. In content sniffing, sniffers change the pattern of the file or change the content to mimic changes in legitimate sites. Content sniffing is also called as media type sniffing or Multipurpose Internet Mail Extension (MIME) sniffing. In this type of attack alteration is made in the stream of bytes, which changes the format of the file. The changed files contain malicious content. Victims can disable this attack by customizing the content of browser option. This type of attack damages the client and server atmosphere [4]. The Process Cycle for Content Sniffing is given in following Fig. 1.

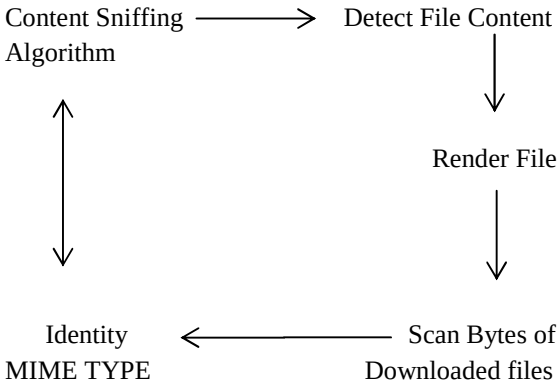

Fig. 1 Process Cycle for Content Sniffing Algorithm

2.5 Password Sniffing: Sniffing is an attack that destroys the confidentiality trait of network security. The main objective of sniffer is to crack passwords and other login information of the victim. The passwords are saved in data packets which are revealed to attackers. The best solution to deal against password sniffing is to use data triggers which manipulate the value of the passwords. If an attacker cracks the confidentiality trait then he can disclose all the data. The main aim of the attacker is to capture the data which is travelling through shared media. If we use one time password or encryption system (It is good solution) attacker will not allow the victim to create a new session because most of the websites browse with both http and https. For example- Attacker stops http link, connection will automatically goes to https which sends all the traffic and creates the entire problem [9]. The flow chart for password sniffing is given in following Fig. 2.

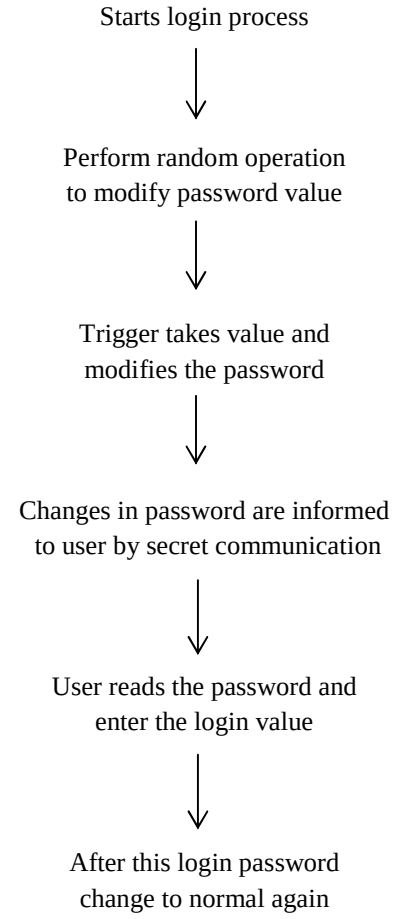

Fig. 2 Process of Password Sniffing

People around the world are now concern about sniffing and they are trying to get rid of it by developing new technologies like - Silver bullets, Tensor Arm, NTUA Snake, etc. These technologies are developed to get rid of mine sniffing. It can operate through various ways like chemical sensation, Robotic eels. Robot kinematics, Snakes work under the main objective of locomotion. With the effective use of these snakes and robots we can make various locomotive patterns like Lateral Undulation, Lateral Rolling, Axial Propagation, Wheeled Rolling, etc. [10].

III. SNIFFING ATTACKS

In this section, various types of web attacks related to sniffing are discussed.

3.1 Phishing: In this type of attack the victim thinks that website is real, but in actual it is the fake website having same domain name. This type of attack is inspired by fishing in which various innocent people become the victim of attacker. The main objective of the attackers is to get the official emails and personal identities of big fat people [2].

3.2 Hybrid Attack: Web attacks are most easily done by attackers and email act as a powerful instrument for attackers, which increases the threat to the users. This type of attack spread malicious emails known as spam [2].

3.3 Shoulder Surfing: In this type of attack, an attacker captures the password by direct observation or by following the individual's activities and their authentication session.

3.4 Bots and Botnets: Bots are computer program that provides various commands and control the system with the help of various kinds of protocols like- HTTP, FTP, Peer-to-Peer protocols. Bots which work on control instructions is known as Botnet. Botnet is a unique combination of robot and network. These are commonly used to destroy computer system. Botnet proves harmful for computer networks as it creates various attacks without the knowledge of victim [4].

3.5 Web Browser Exploits: In this type of attack, attacker creates a websites which is used to perform malicious tasks. This websites helps in finding out the victim's personal information without his permission and he does not have any knowledge of such attack [2].

3.6 Cross-Site Scripting (Xss): This type of attack occurs when the content is not filtered properly and the attacker take this as an advantage by inserting fake Java script and HTML content through invalid inputs which are run by the browsers.[5]

3.7 Attack against TCP/IP: this occurs because protocol makers could not easily get at the level up to which an attacker attacks the internet denial of service attack involves TCP/IP involving interference with natural timing occurs as the connection established, used and after this it is closed [7].

3.8 Denial of Service Attack (DOS): This attack occurs because of different types of tools like TFN (Tribal Flood Network), Trinoo, TFN2K, etc. Various researches concluded that DOS creates serious problem against internet protocol control with an accent on the internet control message protocol and also creates vulnerabilities inner domain of the protocol. The messages are sent by ICMP redirects technique which has very weak security and anyone can easily sniff the address and the message from router, which automatically change the routing tables of the vulnerable computer and all the information will be sent to the attacker's computer [7]. The solution for the security of router is RIP and OSPF mechanisms. By installing the connection, attacker captures all the victim information [8].

3.8 MAC Attacks: This leads to MAC flooding in which numerous requests floods the switch, switches have limited memory so they start sending all traffic out on all ports, so that attacker is able to sniff these traffics in the network.

3.9 DHCP Attacks: In this type of attack, attacker prevent host to use the network by not providing their IP address. They consume the IP address in DHCP format.

3.10 DNS Poisoning: It is also called DNS spoofing or DNS cache poisoning. This is a hacking attack in which data is introduced in domain name system, leading the server to visit an incorrect IP address. In other words, this attack diverts traffic to attacker's computer system. Usually computer uses DNS server which is given by an Internet Service Provider (ISP). To perform this type of attack, attacker exploits a flaw in DNS software.

3.11 ARP Poisoning Attacks: This attack basically targets the traffic which enables an interface on an unsecured network. The Address Resolution Protocol (ARP) is used to resolve to IP address to MAC address. ARP spoofing trust on unauthenticated user, attacker tells entire network that its MAC address is fake similar to IP address of the victim rather than correct MAC to IP mapping. The attacker keeps victim's MAC address in ARP table which prepares data from network host. This 'Man in the middle' attack leads to various other network attacks like Eavesdropping, Replay attacks, Insertion attacks.

IV. RELATED WORK

In 1995, Daniel l. McDonald [13] enlighten the merits of one type pad (OTP) by launching a software named one time passwords in everything (OTP) which diverge from S/key (Password sequence of authentication) during designing. OPI defeats password sniffing attacks. He provided safety from various social engineering attacks like shoulder surfing. Shoulder surfing is basically a technique to maintain view by direct observation to get information [1]. It is commonly used to obtain passwords, PINs, security codes, and similar data.

In 2006, Susan gave information that when user inputs password publically the rate of risk of attacker of stealing password increases. Attacker easily captures the password by following user's authentication process. This is known as shoulder

surfing. Super valiance is the best solution for dealing with shoulder service. Susan developed and evaluated a game like authentication graphical method which is known as convex hull click (CHC). CHC inhibits user to know about graphical password safely in dangerous location as users can easily go to password image. Password sniffing creates lots of problems as transfer of password goes in the same format through communication medium. HTTPS needs secure cover to make encryption sessions during browsing [12].

In 2007, Manu developed an eye password in which a user puts password or pin with the help of keyboard under full vision. This technique is known as gaze-based passwords which require additional time which increases the rate of error [11].

In 2008, Ruichuan Chen [19] developed a poisoning-resistant security framework in which users can only believe on trusted source as it only verifies the integrity of trusted source.

In 2009, Adam Barth [5] provided defense against content sniffing XSS. They construct a model content sniffing algorithm which provides security and also maintains compatibility having four major browsers. Web browser teaches the algorithm to work on the content of HTTP responses and MIME type of the server. If attacker detects this algorithm then he can easily leads to cross- site scripting (XSS) attack. In his study, he found models of this algorithm with the help of four major browsers. Content sniffing XSS attack affects Wikipedia and HotCRP (web application).

In 2010, Zubair M. Fadlullah [14] proposed a detection system against attack on protocols by using Monitoring stubs (MSs). This MSs detect attack and construct a normal file. MSs notify victim server, it trace the origin of the attacker by DTRAB (Detection & Trace Back).

In 2011, Anton Barua [16] launched a Detection system which worked against server site content sniffing attack, by analyzing the content using HTML or Java script. It also checks the activities of browser by doing regular mock download. This detection mechanism results in prevention of uploading malicious files and secure program against this attack.

In 2011, Misganaw Tadesse Gebre [15] proposed a filter that works from the server sites in order to protect browsers who treat non HTML contents as HTML contents.

In 2011, Peiqing Zang [20] analyzed the attacks between user and content owners. This led to information threat.

In 2011, Suhas Mathur [21] studied various approaches in order to prevent content leaking formed by various packet sizes.

In 2011, Brad Wardwin [22] suggested the solution to deal with phishing websites. According to his survey he said that phishers alter their source code which is used in their attacks so that no one can detect their activities.

In 2012, Syed Imran Ahmed Quadri [3] provided security against attack for both client and server sites. In his research paper this security framework provides prevention method for server sites and works from client site. This works against content sniffing attacks. This security is important in order to prevent phishing sites by file splitter technique. The demerit of this framework is that it doesn't work against browser as it treats non HTML files as HTML files. He proposed a security system in order to detect content sniffing in server client relation as it secures server and warn client site.

In 2012, Namrata Shukla [17] presented a model to detect fraud by maintaining a data file which contains the data separated by space, frequency and position. The data is encrypted by substitution method & send it to receiver and detect fraud.

In 2012, Usman Shaukat Qureshi [23] provided modern web applications to internet users by launching AJAX which reloads page and updates only important section of webpages. It consists of large number of important components which deals with HTTP requests, HTML codes, and client & server site scripts. It consists of different layer which provide various threats in web application which leads to large number of attack. For example- Content sniffing attack, Mal- advertising attack, CSR forgery attack, XSS attacks, Man in the Middle attacks and Click jacking attack. They focus on improving security of web application (AJAX).

In 2012, Fokko Beekhof [24] dealt with issues related to identification and authentication of digital based content finger printing. In case of binary content finger printing (Blind attack) random fingerprints of original content are formed which detects the attacker by creating items whose fingerprints are related to the fingerprints of authentic items.

In 2013, Seungoh Choi [25] derived that interest flood attack is applied for denial of service (DOS)

in content centric network (CNN) which results in great quality of service. This results in threats of DOS in CNN.

In 2013, Animesh Dubey [18] proposed a separation technique for various web based, PDF, text, files. This technique works for attack time detection. The main objective of this technique works in two directions in reducing the time and in direction of supporting the file.

In 2013, Bhupendra [2] studied that the client and server environment may have threat from various attacks like Replay attack, content sniffing attack, cross- site scripting attack, denial of service attack, etc. Nowadays content sniffing and cross site scripting (XSS) are the major security threats in server–client relation.

In 2013, Van Lam [26] informed about Drive- by download attacks in which browsers get infected by malicious content send by web servers become a common attack in current years. There are various methods to detect this attack with the help of mining techniques. Each security methods use different features to detect attack. Proper framework is required in this experiment to compare various selection features. Drive-by download attacks are analyzed as it concentrate on the changes happened during browsers rendering information which captures a link between actual and modified streams.

V. ANALYSIS

Various analysis of for reducing password sniffing is observed as:

(a) This is very cost effective as it does not require any costly certification.

(b) This is very less time consuming process as it performs simple and easy results.

(c) This works for both http and https browsing.

(d) It reduces the threat on confidentiality as it stops the disclosure of data from attackers through modifying the databases.

(e) If an attacker sniffs the password than also he was unable to crack the original password and login will not be able for the attacker.

(f) It also works against attacks like shoulder surfing.

VI. CONCLUSION

After studying various research papers, it is concluded that sniffing is a major attack on websites or in other words it is a major threat to browsing. Sniffing attack is very difficult to detect, but once this attack is detected then it can easily be quarantined. It is better to take precautions because it cannot be cured. Various research papers also describe about flash work in which MIME type file can be converted into HTML type. The filters are attached in the network so that it can filter the unauthorized access. Since the security measures are costly so it can't be possible for small scale organization. With the help of triggers it is easy to secure connection for complex authentication also. This prevents attacks like sniffing; shoulder surfing, overhearing, dumpster driving. Passwords having alpha-numeric character are made to secure connection. Various algorithms are used to prevent sniffing. Browser content sniffing algorithms are also used to provide defense against content sniffing XSS. In nutshell, it is concluded that sniffing can be controlled by using different variety of filter for different sniffing attacks.

REFERENCES

[1] V. Mishra and N. Verma, "Security against Password Sniffing using Database Triggers", International General of Research in Advent Technologies, Vol. 2, March 2014.

[2] B. Singh Thakur and S. Chaudhary, "Content Sniffing Attack Detection in Client and Server Side: A Survey", International Journal of Advanced Computer Research, Vol. 3, Issue 10, June 2013.

[3] S. I. A. Qadri and K. Pandey, "Tag Based Client Side Detection of Content Sniffing Attack with File", International Journal of Advanced Computer Research, Vol. 2, Issue 5, September 2012.

[4] S. Pandey and A. S. Chauhan, "Secure Content Sniffing for Web Browser: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 9, September 2013.

[5] A. Barth, J. Caballero and D. Song, "Secure Content Sniffing for Web Browsers or How to Stop Papers from Reviewing themselves"., SP '09 Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, IEEE Computer Society Washington, DC, USA, pp. 360-371, 2009, ISBN: 978-0-7695-3633-0

[6] Z. Trabelsi, H. Rahmani, K. Kaouech and M. Frikha, "Malicious Sniffing Systems Detection Platform", Proceedings of the 2004 International Symposium on Applications and

the Internet (SAINT'04), 0-7695-2068-5/04, 2004

[7] P. Ramakrishna and M. A. Maarof, "Detection and Prevention of Active Sniffing on Routing Protocol", Student Conference on Research and Development Proceedings, Student Conference on Research and Development Proceedings, Shah Alam, Malaysia, 2002

[8] Y. Liu, T. Menzies and B. Cukic, "Data Sniffing-Monitoring of Machine Learning for Adaptive Systems". Proceedings of the 14th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'02) 1082-3409/02, 2002

[9] Simon Baatz, Matthais Frank, Carmen Kuhl, Peter Martini and Chirstoph Scholz," Adaptive Scatternet Support for Bluetooth using Sniff Mode", 0-7695-1321-2/01, 2001

[10] I. A. Gravagne and R. L. Woodfin, "Mine-Sniffing Robotics Snakes and Eels: Fantasy or Reality?" Proceedings of the 5th Intl. Symp. Technology and the Mine Problem, pp. 1-8, Apr. 22-25, 2002

[11] M. Kumar, T. Garfinkel, D. Boneh, T. Winogard, "Reducing Shoulder Surfing by using Gaze-based password Entry", Third symposium on Usable Privacy and Security, ACM society, pp.13-19, 2007.

[12] S. Weidenback, L. Sobrado, J. Camille Birget, J. Waters, "Design and Evaluation of the Shoulder Surfing Resistant Graphica password scheme", Conference on Advanced visual interfaces, ACM society, pp. 177-184, 2006.

[13] D. L. Mc. Donald, R. J. Atkinson, C. Metz, "One Time Passwords In Everything(OTPE) Experiences with Building and Using Stronger Authentication", Proceedings of the Fifth USENIX UNIX Security Symposium, 1995.

[14] Z. M. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani and N. Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols through Traffic-Feature Analysis", IEEE/ACM Transaction On Networking, Vol. 18, No. 4, 2010.

[15] M. T. Gebre, K. Lhee and M. Hong, "A Robust Defense against Content Sniffing XSS Attacks", In Digital Content, Multimedia Technology and its Applications (IDC), 2010 6th International Conference on, pp. 315–320. IEEE, 2010.

[16] A. Barua, H. Shahriar, and M. Zulkernine, "Server Side Detection of Content Sniffing Attacks", 22nd IEEE International Symposium on Software Reliability Engineering, 2011.

[17] N. Shukla, S. Pandey, "Document Fraud Detection with the help of Data Mining and Secure substitution Method with Frequency Analysis", International Journal of Advanced Computer Research (IJACR), Volume 2 Number 2, 2012.

[18] A. Dubey, R. Gupta, G. S. Chandel, "An Efficient Partition Technique to reduce the Attack Detection Time with Web based Text and PDF files", International Journal of Advanced Computer Research (IJACR), Volume-3 Number-1 Issue-9, 2013.

[19] R. Chen, E. K. Lua, J. Crowcroft, W. Guo, L. Tang and Z. Chen, "Securing Peer-to-Peer Content Sharing Service from Poisoning Attacks", Eighth International Conference on Peer-to-Peer Computing, 2008.

[20] P. Zhang, B. E. Helvik, "Modeling and Analysis of P2P Content Distribution under Coordinated Attack Strategies, 7th IEEE International Workshop on Digital Rights Management Impact on Consumer Communications, DRM, 2011.

[21] S. Mathur and W. Trappe, "BIT-TRAPS: Building Information-Theoretic Traffic Privacy into Packet Streams", IEEE Transaction on Information Forensics and Security, Vol. 6, No. 3, 2011.

[22] B. Wardman, T. Stallings, G. Warner, A. Skjellum, "High-Performance Content based Phishing attack Detection", ecrime Researchers Summit (ecrime), 2011, vol. 1, Issue 9, pp. 7-9, 2011.

[23] U. S. Qurashi, Z. Anwar, "AJAX Based Attacks: Exploiting Web 2.0", In proceeding of International Conference on Emerging Technologies (ICET), IEEE, 2012

[24] F. Beekhof, S. Voloshynovskiy, F. Farhadzadeh, "Content Authentication and Identification under Informed Attacks", Proceedings of IEEE International Workshop on Information Forensics and Security, Tenerife, Spain, 2012

[25] S. Choi, K. Kim, S. Kim, and B. Roh, "Threat of DoS by Interest Flooding Attack in Content-Centric Networking", International Conference on Information Networking (ICOIN), Bangkok Thailand, pp.315-319, 2013

[26] V. Lam Le, I. Welch, X. Gao, P. Komisarezuk, "Anatomy of Drive-by Download Attack",

Proceedings of the Eleventh Australian Information Security Conference (AISC 2013), Adelaide, Australia, 2013.