# Session Clocking Attack Detection and Defense Strategy on TCP Session in Network

Sandip Khote
DYPCOE, Pune

Amar Shinde
DYPCOE, Pune

## ABSTRACT
TCP-IP model is the most widely used model in internet now days. Security is the most promising thing in online work. In these paper we are introduced some attacks on TCP Session. Attacks like Session hijacking, Session Clocking, and IP sniffing. As well as we introduced some methodologies how to dealing with these attacks.

## Keywords
Session, session hijacking, ip spoofing, session clocking, network security.

## 1. INTRODUCTION
Now a days Internet is the very important Thing in Human Life. Nobody can imagine world without an Internet. All over world people can make use of Internet for their work. For various purposes of human make use of Internet like Knowledge, Entertainment etc. Some normal or daily activities like pay online bills, online banking, online mobile recharge, online shopping etc. Most Prominent use of internet on today is E-commerce. In all over world e-learning is the most useful technique in universities. Another aspect of internet is Ubiquitous computing. Ubiquitous computing means computer is hiding from user. Although there are various uses of internet but some misuse is also done.

## 2. MOTIVATION
Using Internet peoples can done their work easily. And saves their time, moneyetc. but some faulty people or attackers make misuse of these facility. The internet provided services to user for communication; online transaction etc. attacker can use it to establish connection with victim now days use can share their personal information on network as well as data. Which caused, facilitate crime on and off the internet. Session hijacking is one of the mostly used attacks on internet, but today there are some techniques to prevent it. The newly introduced technique is Session Clocking attack on Internet.

## 3. RELATEDWORK
Sheng Pang [2] proposed technique to detect Session hijacking by using ping command. In this paper he compares the TTL value the send packet and ping command.
Yongle Wang [3] has proposed techniques to prevent spoofing attack. He has given various methods to prevent spoofingattack in TCP/IP session.Enlightened us with information about spoofing attack. He has also informed us about packet sniffing by setting MAC Address and IP Address to coincide with Gateway and sending away packets.There is property of TCP/IP header that TTL values is increased more than the value in which is average TTL value the packet will discarded and the request for network packet will send

## 4. SESSION
Session is temporary establish connection between two or more computer and devices for communication, sharing information.

## 5. PING
PING is a computer network administrator tool used to test the reach ability of a host on an internet protocol network and to measure the RTT (Round Trip Time) for packets sent from the source to destination computer. The name of ping was defined by active sonar terminology which sends a pulse sound and listens for the echo to detect objects underwater.

## 6. SESSION HIJACKING
Session hijacking is also known as "COOKIESHIJACKING". The first attack was done in 1994.When HTTP 0.8 was introduced in earlier version session hijacking was not possible. The goal of attacker is to create circumstances where the client and server are unable to exchange data so that he/she can grabs the packets for both ends and which interchanged the real packets .thus he/she was able to gain access of session

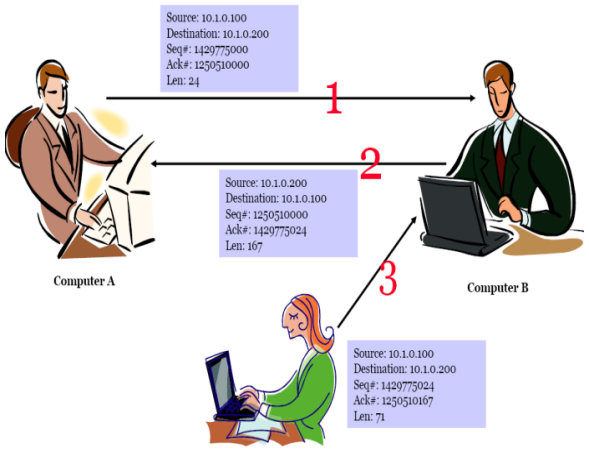


**Fig 1**: **Concept of Session Hijacking**

## 7. SESSION CLOCKING
Let us discussing session clocking first we will give concentration on Packet Sniffing.

### 7.1 Packet Sniffing
It is a technique of monitoring the packets that transferred between networks. A packets sniffer is a piece of software or hardware that monitors all network traffic. The security functions presented by sniffer is their capability to monitors all incoming and outgoing traffic including clear-text password and username or other sensitive data. Sniffing takes part in capturing, decoding, and interpreting the information inside the network

### 7.2 Session Clocking
Session clocking attack is the combination of sniffing and spoofing attack. The name used as session clocking because the attacker manages the attack on time and session issue so we identify this attack is session clocking attack. This attack is done on live network, hacker can check the authentication

session to change it on going network or to sniff packet. Hacker use advanced technique and strategy to anonymously attack the network without any detection. Because of clocking attack there is risk of losing data completely. This attack.Mostly harmful to online banking, online shopping etc.

# 8. PROPOSED SYSTEM

In the First method of detection it is very promising task to detect clocking on network, there are very few utilities that give a clue to possible sniffer presence. There are two way to identify a sniffing,

1. Host based
2. Network based

## 8.1 Host based Detection

In host based detection we can use some function or parameters to detect if NIC is running in promiscuous mode on any host in annetwork. Since the basic requirement for sniffer to work is to put the NIC in the "Read All" mode disabling it can very effectively help shutting down stray sniffers.

## 8.2 Network Based Detection

In these systems anti-sniffer software can be used to detect the presence of specific signature of packets. We can use another utility some scripts can be operates to check each network host for the presence of known sniffer, processes etc. Some modern antivirus or antispyware software is capable of detecting sniffing software. This test is also run during the flood of traffic. It contains sending large amount of ICMP echo request messages to host. It keeps track of number of dropped ping responses. In the proposed system second method is protection. The very important field while design a light perimeter defense system while generating network architecture. Disable promiscuous mode on network interface in shutdown most sniffer software. This can be done by running an admin script as a daily job on network or deploying a network policy at the host level to control access to the network card configuration networkIn proposed system we can study different we can study different TCP/IP fields, we modified some field to make packet more secure than existing system. We will detect attack by using ping command in TCP field as the packet it being on a ping command will be triggered and at same time attack will be detected. There is property of TCP/IP header that TTL values is increased more than the value in which is average TTL

# 9. CONCLUSION

Session Clocking Attack is advanced type of technical attack made by the attackers. But to developed socket programming code to detect purpose, we can detect this attack using method -1 technique. Also, using TCP packet along with the ping command we can detect session clocking attack.

Prevention of these types of attacks can be carried out by the property of the TCP/IP which discards the packet.

Technique of regeneration of session IDs & encryption will also be helpful for this prevention (future work).

# 10. REFERENCES

[1] Richard Clayton, et. "Ignoring the Great Firewall of China", Volume 4258/2006 Privacy Enhancing Technologies

[2] Sheng Pang; Changjia Chen; Jinkang Jia, "Session Hijack in the Great Firewall of China," Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09.International Conference on, vol.1, no., pp.473, 476, 25-26 April 2009

[3] Yongle Wang; JunZhang Chen, "Hijacking spoofing attack and defence strategy based on Internet TCP sessions,"

[4] Dhar Sumit. "Switch Sniff." (March 5, 2002)*2nd International Symposium on,* vol., no., pp.507, 509, 23-24 Dec. 2013

[5] Ettercap. "Ettercap." (May 11, 2003)

[6] Graham, Robert. "Sniffing (network wiretap, sniffer) FAQ." (September 14, 2000)*Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013*

[7] https://www.owasp.org/index.php/Session_hijacking_attack

[8] http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html

[9] http://stackoverflow.com/questions/22880/what-is-the-best-way-to-prevent-session-hijacking

[10] http://luizfirmino.blogspot.in/search/label/Session%20Hijacking

[11] http://www.linuxjournal.com/article.php?sid=5869

[12] http://www.robertgraham.com/pubs/sniffing-faq.html

[13] http://ettercap.sourceforge.net/