**Case Study: Session Hijacking**

Name

Institution

Professor

Course

Due date

**ABSTRACT**

This document will introduce chat hacking, explain its process, how it differs from spoofing, and the steps to take to stop chat hacking. I will also follow the prediction.

Session hijacking is a network attack technique that allows an attacker to hijack another user's session. An attacker can access a user's account, personal information, or other sensitive information without the user's knowledge or permission. Session hijacking can be done by hijacking network traffic, stealing session cookies, or infecting the user's computer with malware. Session hijacking can be prevented by using strong passwords, multi-factor authentication, VPNs, and keeping software updated. (Baitha, A.K. and Vinod, S. (2018))

Sequence number prediction is the task of predicting the next number (Qian Zhiming, Mao Zhiming, Xie Yang (October 2012))

*Key words:* session hijacking, spoofing(deception),sequence number prediction

**What happens when a session is hijacked?**

A session (chat )hijacking attack occurs when an attacker impersonates an online user via chat. This allows the attacker to access the user's account, information, and actions on the website or app. For example, an attacker can withdraw money from the user's bank account, make purchases using their credit card, or reset the password.

Session hijacking attacks can occur when an attacker captures a user's session ID (a unique number used by a website or application to track a user's activities). The session ID is usually stored in a cookie, URL, or a hidden location on the website. Attackers can use a variety of techniques to obtain session IDs, such as hijacking network traffic, guessing the session ID, or tricking users into clicking malicious links.

 To prevent session hijacking, users should avoid using public or unsecured Wi-Fi networks, exit websites or applications after use, and use an HTTPS connection whenever possible. Websites and applications should use secure session management techniques such as encrypting session IDs, creating unique and anonymous session IDs, and setting timeouts.

**Difference between spoofing and hijacking**

Spoofing and hijacking are cyber attacks that involve impersonating someone or something on the internet. But they have some important differences:

Spoofing is when an attacker impersonates a trusted source (such as a website, email, or IP address) to impersonate a brand intending to provide information or business. For example, an attacker could set up a fake website that resembles a real bank's website and ask the target to access login information. (Schuckers, S. C. (2002))

Hijacking is when an attacker takes control of an existing online session or connection (such as a browser, web application, or network) and gains access to the target account, information, and performance. For example, an attacker could capture a target's session ID (a unique identifier that identifies a user on a website) and use it to access their account and conduct business. (Bugliesi, M., Calzavara, S., Focardi, R. Khan, W. (2015))

Spoofing and interception can have serious consequences for targets such as identity theft, financial loss or deletion of information. To protect against these attacks, users should use secure and up-to-date devices, networks, and software and be careful about what they click, download, and type online. Websites and applications must use secure session management and encryption techniques and verify the identity and integrity of sites and sites.

**Steps to Perform a Session (Chat) Hijacking Attack**

A chat hijacking attack is a type of cyber attack that involves taking control of other users' systems. chat online and do it yourself. The main steps to stop chat hijacking are: (Bugliesi, M., Calzavara, S., Focardi, R. and Khan, W. (2015))

**- Step 1: Look for the purpose of the discussion.**

Attackers need to find users who are logged into the website or application they want to access. Attackers can use a variety of methods to find targets, such as network analysis, phishing or social engineering.

**- Step 2: Steal the session ID.**

The attacker must obtain the target user's session ID, which is a unique number used by the website or application to identify the user. The session ID is usually stored in a cookie, URL, or a hidden location on the website. Attackers can obtain session IDs using a variety of methods, such as hijacking network traffic, guessing session IDs, or tricking users into clicking malicious links.

**- Step 3: Skip the session.**

The attacker must use the time to steal the identity to control the target user's session. Attackers can obtain stolen identities by changing their cookies, URLs or passwords, or by using tools that allow them to reject session IDs. An attacker can log into a website or application as a user and do anything the user can do, such as steal data, trade, or change domains.

**- Step 4: Control the speech.**

 The attacker needs to keep talking and avoid getting caught. The attacker can achieve this by copying the behavior of the target user, avoiding strange behavior and changing the session ID when they are vulnerable. Attackers may also attempt to prevent targeted users from logging out or viewing hacked content by blocking their access, deleting their notifications, or sending their messages. Please go somewhere else.

**Session Hijacking differences**

Session hijacking is a type of cyber attack that involves taking control of other users' online sessions and harming them. There are different types of session hijacking depending on whether the attacker uses a session ID, which is a unique identifier that identifies the user of the website or application. (Dacosta, I., Chakradeo, S., Ahamad, M. Traynor, P. (2012)) Here are some types of session hijacking:

**Network level hijacking:**

 Commenter sniffing uses the network running between select the domain and server and get the session id from the server. An attacker can use the session ID to log into the user's session. This hacking can be prevented by using encryption and security protocols such as HTTPS and SSL.

**Application-level hijacking:**

An attacker exploits a weakness or bug in a website or application to create malicious code or script that can obtain session IDs from the user's browser or device. An attacker can use the session ID to log into the user's session. This hacking can be prevented by using safe coding techniques such as checking input, sanitizing output, and executing special characters.

**Session pinning:**

The attacker gives the user the session ID before logging in and asks the user to use the session ID. An attacker can use the same session ID to log into client sessions. This hacking can be prevented by using a unique and unknown session ID and changing the session ID after the user logs in.

**Session side hijacking:**

The attacker obtains the session ID from the client cookie, which is a small cookie that stores the browser user's session ID. An attacker can use the session ID to log into the user's session. This hacking can be prevented by using secure cookies, encrypting them, and setting the cookie expiration date.

**Sequence (Ordinal) Number Prediction**

Ordinal Number Prediction is the task of finding the next value in a sequence of numbers based on the previous value and some pattern or method. law. For example, if the array is 2, 4, 6, 8, the additional value is 10 because the array follows the rule of adding 2 to each element.

 Serial numbers can be useful in many applications such as cryptography, network security, data compression and pattern recognition. (Jhaveri, R.H., Desai, A., Patel, A.zhong, Y. (2018))

There are many methods to estimate numbers depending on the type and complexity of the sequence. Some methods are:

**Linear Regression:**

 This method assumes that the sequence follows a relationship such as y = ax + b; where y is the array value, x is the array, and a and b are. is fixed. This method tries to find the best value of a and b to minimize the error of the actual and predicted values. For example, if the sequence is 3,5,7,9, the horizontal line will find a = 2 and b = 1 and predict the next value will be 11.

**Polynomial regression:**

This continues with the output of the line leading to higher order polynomials such as y = ax^2 + bx + c; where y is the row value, x is the row index, and a, b, and c are constants. This method tries to find the best value of a, b, and c to minimize the error of the actual and predicted values. For example, if the sequence is 1, 4, 9, 16, polynomial regression finds a = 1, b = 0, c = 0 and predicts the next value will be 25.

**Exponential Regression:**

This method assumes that the sequence follows a relationship such as y = ab^x; where y is the array value, x is the array index, and a and b are regular parameters. This method tries to find the best value of a and b to minimize the error of the actual and predicted values. For example, if the sequence is 2,4,8,16, exponential regression will find a = 2 and b = 2 and predict the next value will be 32.

**Neural Networks:**

 This uses the following computational models: it replicates the structure and function of biological neurons and can learn arbitrary patterns from data. This method takes time and gives a prediction of the next price depending on the input. This method examines the parameters of the model by varying the error between actual and predicted. For example, if the sequence is 1, 1, 2, 3, 5, 8, the neural network method will learn the Fibonacci rules and predict the next value will be 13.

 These are just a few examples of serial number predictions.There are many methods in Markov model, hidden Markov model, recurrent neural networks, etc., which can solve different types of connection and prediction problems.

**Conclusion**

An attacker can steal user time and access data or resources without permission laws by exploiting a weakness in TCP connection codes. This is called session hijacking. (Bugliesi, M., Calzavara, S., Focardi, R. and Khan, W. (2015)). TCP connects to the network and sends packets.

Here are some ways to prevent session hijacking:

*  Use methods that encrypt and authenticate data, such as SSL/TLS or SSH
*  Generate a random and unthinkable initial sequence number
*  Using firewalls and intrusion . Internet Traffic Monitoring and Filtering System
*  Educate users about the dangers of using unsecured networks or clicking on suspicious links.

Session hijacking and sequence number guessing can compromise the security and privacy of online users and systems. Therefore, it is important to understand the methods and tools used by attackers and use the necessary protection to prevent attacks.

**References**

Baitha, A. K., & Vinod, S. (2018). Session hijacking and prevention technique. *Int. J. Eng. Technol*, *7*(2.6), 193-198.

Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. (2012). One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. *ACM Transactions on Internet Technology (TOIT)*, *12*(1), 1-24.

Bugliesi, M., Calzavara, S., Focardi, R., & Khan, W. (2015). CookiExt: Patching the browser against session hijacking attacks. *Journal of Computer Security*, *23*(4), 509- 537.

Hossain, M. S., Paul, A., Islam, M. H., & Atiquzzaman, M. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. *Netw. Protoc. Algorithms*, *10*(1), 83-108.

Jhaveri, R. H., Desai, A., Patel, A., & Zhong, Y. (2018). A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs. *Security and Communication Networks*, *2018*, 1-13.

Qian, Z., Mao, Z. M., & Xie, Y. (2012, October). Collaborative TCP sequence number inference attack: how to crack sequence number under a second. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 593-604).

Schuckers, S. A. (2002). Spoofing and anti-spoofing measures. *Information Security technical report*, *7*(4), 56-62.