**Case Study: Session Hijacking**

Name

Institution

Professor

Course

Due date

**ABSTRACT**

This document will introduce session hacking, explain its process, how it differs from spoofing, and the steps to take during a session hacking attack. I will also make a sequence number prediction.

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

Session hijacking is a type of attack that uses a web session control mechanism that is normally managed by a session token. A session token is a string of data that identifies a user and allows them to remain authenticated and logged in to a website or application. A session hijacker can steal or guess a valid session token and use it to gain unauthorized access to a user's account or information. 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 user activity).(Baitha, A. K., & Vinod, S. (2018))

**Differences between spoofing and hijacking**

Spoofing and hijacking are related but different concepts.

Spoofing is the act of pretending to be someone else, for example by changing the source IP address or email address of a message.

Hijacking is the act of taking something that belongs to someone else, such as a session, connection, or device.

Spoofing can be used as a technique to facilitate hijacking, but not all spoofing attacks lead to hijacking.(Schuckers, S. A. (2002))

**Steps in Performing a Session Hijacking Attack**

The steps involved in performing a session hijacking attack can vary depending on the type and method of the attack, but generally include the following stages:

- Session monitoring: An attacker monitors network traffic and tries to find an active and authenticated session between the user and the server.

- Session Analysis: The attacker analyzes the session token and tries to figure out how it is generated and transmitted. An attacker can use a sniffer or proxy tool to capture and inspect the session token.

- Session theft: An attacker obtains a session token using various techniques such as session monitoring, session prediction, session fixation, or cross-site scripting. An attacker can also try to force the user to log out or expire the session in order to obtain a new and predictable session token.

- Session Exploitation: An attacker uses a stolen session token to impersonate a user and access their account or information. An attacker may also attempt to elevate their privileges or perform malicious actions on behalf of the user.

(Hossain, M. S., Paul, A., Islam, M. H., & Atiquzzaman, M. (2018))

**Types of Session Hijacking attacks**

There are different types of session hijacking attacks depending on the layer of the network protocol stack where they operate. Some of the common types are:

- Network-level hijacking: An attacker hijacks a TCP connection between a user and a server by guessing or manipulating TCP sequence numbers. This allows an attacker to insert, modify, or delete packets in communication.

- Application-level hijacking: An attacker takes over a web session between a user and a server by stealing or guessing an HTTP session token, such as a session cookie or a URL parameter. This allows an attacker to access the web application as a user.

- 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.

(Hossain, M. S., Paul, A., Islam, M. H., & Atiquzzaman, M. (2018))

**Sequence number prediction**

Sequence number prediction is a technique used in network-level hijacking where an attacker tries to guess the next TCP sequence number to be used by a user or server when communicating. This allows an attacker to inject packets into a TCP stream without breaking the connection. An attacker can use various methods to predict the sequence number, such as brute force, sampling, or clock bias analysis.(Qian, Z., Mao, Z. M., & Xie, Y. (2012, October))

To perform sequence number prediction, you must have access to the network traffic between the user and the server and be able to capture and analyze TCP packets. You also need to know the algorithm and parameters used by the TCP implementation to generate sequence numbers. You can then use a tool or program to simulate the algorithm and try to compare the observed sequence numbers. Once you have a match, you can predict the next sequence number and use it to create a packet to be received by the user or server.

There are some tools and programs that can help you predict the sequence number, such as Nmap, Hping or Scapy.(Jhaveri, R. H., Desai, A., Patel, A., & Zhong, Y. (2018))

There are many methods of predicting 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 finds a = 2 and ab = 1 and predicts that the next value will be 11.

* + Polynomial regression:

This continues by outputting a 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 that 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 finds a = 2 and b = 2 and predicts that the next value will be 32.

* + Neural Networks:

It uses the following computational models: it replicates the structure and function of biological neurons and can learn arbitrary patterns from the data. This method takes time and provides a forecast of the next price depending on the input. This method examines the model parameters 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 rule and predict that the next value will be 13.

**Conclusion**

Session hijacking and serial number guessing can compromise the security and privacy of online users and systems. Therefore, it is important to understand the methods and tools that attackers use 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