Vulnerabilities and Prevention of Session Hijacking

Taylor Charles

East Carolina University

This article will assess the technological issue of session hijacking in regards to exposing all of its vulnerabilities as well as provide ways to prevent session hijacking. Session hijacking occurs when someone has unauthorized access and gains the ability to hack into the information or services of a computer. Consequently, many people are unaware of this kind of attack and lose valuable, sensitive information every day. Each time someone is using the web browser, there are cookies that are being used to authenticate the user. A hacker has access to many different tools that aid their hacking behaviors such as sniffing; a cross-sit script attack, and the “man-in-the-middle attack.” Since technology is considered the lifeline of our current society, it is urgent that there be better protections for the large companies, small businesses, and personal users of the Internet. Money travels constantly through network sessions through banking, online payments, and online shopping, which is one reason why hacking has become a huge issue in the technological world.

Session hijacking is TCP based and has the advantage of interfering in real time, during the active session. Sometimes the intrusion can be blocked depending on the level of knowledge the innocent user has to prevent the attack. If a website does not respond to one’s credential information used to access their information within a site, it is possible that someone could initiate a session hijack during that time window. Therefore, there are steps that a person can follow to avoid this situation. One step to use SSL and HTTPS encryptions for websites, which makes the hacking effort more complicated than the hacker may be able to handle. Another method involves the users deleting the cookies of their sites in order to help prevent other hackers from obtaining their log in information. This is a very good practice that can be done at any time before or during the network session by the user.

As technology networks expand and improve, the ways that a user can be hijacked multiply. Due to the potential dangers of this issue, it is essential that users become aware and comfortable with the vulnerabilities of their web sessions and have the knowledge to know how to prevent or reduce these instances. A hacker can initiate an attack almost anywhere at any time where a web session is available. For example, an individual may be in public place like the store, coffee shop, or mall with their electronic device. Thousands of people connect to public Wi-Fi daily, also known as Hot Spots. People are unaware of how vulnerable public networks are. Various business people use sensitive information on these networks on a daily basis.

Hackers are aware of all the public access to hotspots and take advantage by hijacking their sessions and obtaining their information. When an individual is connected on a network there are different steps that take place that enables communication to web servers. Also, when a client PC is trying to contact a web server it uses the TCP 3-way handshake to authenticate the communication. A client first sends contacts to a server by sending a SYN (Synchronize) packet. Their server responds with a SYN/ACK packet that has a unique number and an ACK number from the originals client's PC. An ACK (acknowledgement) packet is sent back to the server to start exchanging data. For example, when a user connects to the Internet, they have a unique session ID to validate their self to the web server in order to establish communication.

When a professional hacker can see the session ID of the victim, the hacker becomes much more powerful than the user may know. A hacker can use session sniffing to obtain the user's ID. Once the hacker obtains the ID of the user, the hacker has just as much access to the network that the user is accessing. However, this is not the only form of attack that can be executed. A hacker can also implement a cross-site script attack. With this attack, hacker compromises the session token by using a malicious code. For example, an attacker will send a crafted link to the victim with malicious JavaScript coding. When the victim clicks the link the script will launch with buttons and steps, which can expose your session ID. Many people are unware of these vulnerabilities this is why people are constantly hijacked daily.

In addition, a hacker also can use the man-in-the-middle attack to intercept the communication between a client and the web server without alerting the user. This attack happens often over any Wi-Fi access point that has no encryption. In order to initiate this attack, it requires the attacker to hijack the client session cookie. A cookie is used to authenticate the user and session for communication. After obtaining the client session cookie, the attacker can pose as the victim with all user privileges and the hacker can modify information before the original packet is sent back to the other user or webserver. Users must realize that it is important to be careful on websites that only support HTTP. HTTP is not secure which makes it a weakness to the user and advantage for a hacker. According to Dacosta, Chakradeo, Ahamad, and Trayno (2012), in their article “One Time Cookies…, state that, “inherent security weaknesses allow attacks against the intergrity of Web sessions.” This statement suggests that HTTPS is recommended over HTTP because it encrypts the website and provides a more secure session. SSL is another way to encrypt to keep the session secure. SSL (secure socket layer) provides a secure connection between browsers and websites, which allows users to transmit private data online. You can spot if SSL is being used in the browser’s URL. SSL is commonly used throughout companies to protect their customers from a session hijack.

Exploit kits such as Firesheep, DroidSheep, CookieCadger and WhatsApp sniffer are common avenues used by hackers. Since there are so many gateways for an attack, the best method is to only use Wi-Fi that has encryption to start off with. Having encryption is having some type of protection so information will not be in plaintext format. SSL and HTTPS are the most effective in the prevention of sniffing and these formats help secure and encrypt information as it is being transferred. Unfortunately, there is no way to guarantee session hijacking will not happen on any network. Even with encryption there are always loopholes that can lead to stealing a user's session but nevertheless, using encryption can make it very challenging for a hacker to obtain.

Firesheep, a session vulnerability in particular, is a common attack that has been dealt with for years now. Firesheep is an extension for the Firefox browser that uses a packet sniffer to retrieve unencrypted cookies from websites. This application monitors and analyzes traffic from a router and any end users that are connected to the network. It is very user-friendly, meaning that anyone using unsecured Wi-Fi can hijack a user's session. As a result, online encrypted end-to-end websites such as HTTPS or SSL can provide protection from Firesheep. Furthermore, sessions can be tracked from cookies, URL Rewriting, and Hidden Fields. A cookie is stored a hard disk. A server verifies the same cookie before processing the request.

Moreover, there is another positive aspect of hacker prevention called URL Rewriting. URL Rewriting can make session tracking more difficult but takes the SID value and goes with the URL of each request to track the session. Finally, Hidden fields are hidden from the user and can be viewed at the page source. They carry SID values that are stored in the hidden fields that can be used to track a session (rarely used). XSS (Cross site Scripting) attacks are very common. According to authors Wurzinger, Platzer, Ludl, Kirda, and Kruegel (2009), "Cross-site scripting (XSS) continuously leads the most wide-spread Web application vulnerabilities lists." A XSS attack allows the hacker to perform a script on the victim's browser. All the attacker has to do is write a script to access the cookie value and send it to a server for the attacker to able to access the user account.

Overall, here are several steps one can take to prevent a session hijack. Users can modify their session ID to make it longer and more difficult for hacker to obtain. Additionally, regenerating sessions prevent session fixations that makes it impossible for the hacker to know what the ID is after the user has logged in. Session fixation is an attack in which a hacker hijacks a valid session. The attack shows the web application session ID. Some services will change the session cookie every request so that it will eliminate the probability of hackers trying to capture your session. Investing in virus protection and malware prevention can help with protecting a user's computer from a session hijack by creating walls and making it tougher on the hacker. Virus protection and malware prevention can easily be purchased online or through disks in local stores and this option is convenient for the user. However, these protections need to be updated when prompted due to the adaptions to the changing network systems.

In essence, it is very important to have security in any business or personal network. The Internet can be very beneficial to users in so many ways yet it can be the place where they lose their identity. With the expansion of technology in society especially in regards to banking, medical records, education, and shopping, the Internet has become the beacon of life for various companies and a convenience for many individuals. Whether it is sniffing, the man-in-the middle attack, or even the cross-script attack, a hacker is waiting around the corner to take a user's identity or personal information. Having protection and encryption is the key to safety from many hackers that live to take away information from individuals. Before browsing a website, a user should always look to make sure if the website is secure with HTTPS or SSL. Taking simple steps like downloading virus protection and malware prevention or deleting cookies before and after network sessions can make a user feel much safer from the eyes of a hacker.