Cole Ramos

IST590-Instuctor Anastacia Webster

May 18, 2018

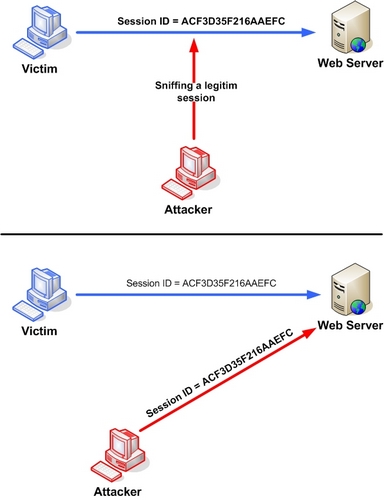
**Session Hijacking**

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.

Because http communication uses many different TCP connections, the web server needs a method to recognize every user’s connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition. (OWASP)

**Example 1-Session Sniffing**

In the example, as we can see, first the attacker uses a sniffer to capture a valid token session called “Session ID”, then he uses the valid token session to gain unauthorized access to the Web Server. (OWASP)



Big websites and servers with many connected computers and visitors are the ideal targets for session hijacking, because the attacker can blend in with the great amounts of traffic and stay hidden in the background.

Forums, banking websites, online shops, are all viable targets and profitable. (Heimdalecurity)

There is a technique that uses engines which fingerprints all requests of a session. In addition to tracking the IP address and SSL session id, the engines also track the http headers. Each change in the header adds penalty points to the session and the session gets terminated as soon as the points exceeds a certain limit. This limit can be configured. This is effective because when intrusion occurs, it will have a different http header order.

These are the recommended preventive measures to be taken from both the client and server sides to prevent the session hijacking attack. (Interserver.net)

In conclusion secure session tracking should not rely on either cookies or ssl session-ids alone, but rather a combination of these two plus many more factors. **Airlock detects and prevents session hijacking by continuously checking this fingerprint of a user’s requests. (techzone)**

References

<https://www.owasp.org/index.php/Session_hijacking_attack>

<https://heimdalsecurity.com/blog/session-hijacking/>

<https://www.interserver.net/tips/kb/session-hijacking-prevent/>

https://techzone.ergon.ch/client-security