#### **Purpose**

This assignment asks you to share your understanding of certain weaknesses in session management after you read the textbook, lecture notes, and other supplementary reading materials.

#### **Tasks**

To make the discussion concise, please focus your discussion on the following questions. Please submit one original post using the following guideline:

* After we explored the lifecycle of session management, we know that web sessions managed by session tokens or identifiers that are automatically generated by a web server are extremely vulnerable if no other session protection is implemented. Please provide an example to show the weakness. Your (imagined or real) example can come from anywhere as long as no organization identity is exposed.
* If you were the designer of the application in your example, how would you fix it?

**Grading Rubric (Total of 3 points)**

1. An uncovered session management weakness and its fix? (1.5 points)
2. The quality of your explanation? (1.5 points)

Example:

An example of session tokens that were generated by a server being exploited by a hacker happened to a well known Youtuber, Linus Tech Tips. This is a well documented event, by the victim as well[1], so I don’t think that revealing identifying information is a problem. A person or persons were able to use some social engineering to get a video editor to open a pdf file attached to an email that contained executable code that was able to access locally stored browser data, such as usernames, passwords, and cookies. The hacker was able to trick the server into believing they were a valid user. During the time the hacker had access to the system, they were able to delete all of the uploaded videos as well as begin to stream their own content which could’ve been (or actually was) used to deceive his audience. Once the victim identified someone had unauthorized access to their system, it took much longer to solve the problem because there was no easy way to clear all active sessions and token information.

Solutions:

There are a couple methods that can be used in tandem to increase security. First, as a user, especially if multiple people have access to an account or service, phishing awareness should be done frequently. This can mitigate many different forms of attempts of someone gaining unauthorized access. Now, from the application side, there are a few tools that can be implemented to make it easier to at least regain access once unauthorized access has been identified. This includes tools that can invalidate all sessions and MFA tokens. This way the proper user can immediately clear all access and selectively re-enable for those who should have access. Another way to mitigate risk is for account access to be highly customizable. In this specific case, an editor account doesn’t need access to video management (delete, upload, start stream, etc..). This way, if a hacker gains access to that account, their reach is limited to the account[2]. Of course, this doesn’t necessarily prevent someone from hijacking a session, but it does highlight that even high security web applications are still penetrable. These solutions will help defend and protect against intruders who have gained access.

References:

1. <https://www.youtube.com/watch?v=yGXaAWbzl5A>
2. https://infosecwriteups.com/linus-tech-tips-youtube-hijacking-highlights-the-importance-of-customizable-permissions-and-bf554470173c