SESSION HIJACKING, ATTACK AND DEFENSE

Enida Puto[1], Kozeta Sevrani[2]

[1]Bank of Albania. Email: enidaputo@yahoo.com
[2] Faculty of Economy, UT, Albania. Email: kozeta.sevrani@unitir.edu.al

Abstract

Session hijacking, sometimes also known as cookie hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network. Successfully hijacking a network session depends on a few conditions falling into place, so an attacker has several tricks and techniques for creating these conditions. The most common ways to compromise a session token are: Predictable session token; Session Sniffing; Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc); Man-in-the-middle attack; Man-in-the-browser attack. Protecting network sessions that carry sensitive and important data such as credit card numbers, bank transactions, and administrative server commands is an important step at improving the security of an organization. By removing an attacker's ability to inject data into those sessions, the security bar is raised and the adversary is forced to try other, more complex avenues that are less likely to compromise the organization's security. In his paper are explored some of the techniques of session hijacking of web applications and are taken several examples of session hijacking through these different techniques. There are explored some of the vulnerabilities that make session hijacking an easy process for attackers and there are mentioned the methods to prevent these kinds of attacks. Later on this paper there are made several conclusions about the defense from these attacks. Because session hijacking works by taking advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter, some of the methods to prevent session hijacking include: Encryption of the data traffic passed between the parties by using SSL/TLS, in particular the session key; Regenerating the session id after a successful login; setting a session timeout etc.

Keywords: *session, hijacking, unauthorized, access, attack, security*