Abstract

Session hijacking is also called as cookie hijacking in which the attacker exploits a valid computer session sometimes also called a session key or session token to get an unauthorized access to user system or back-end server. So to prevent this type of attack we are creating a protocol that will prevent the attacker from gaining the access of encrypted cookie and back-end server. We are developing a Reverse proxy server (RPS) with a One Time Cookie (OTC) and generating a browser fingerprinting, IP address of system, session ID such that Reverse Proxy server handles a request using One Time Cookie (OTC) protocol to prevent adversary from capturing and injecting the session credentials also we are using Blowfish Algorithm for the encryption purpose. If any of this parameter alter than we can be easily identified the attacker.

References

1. Willem Burgers, Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials, in Institute for Computing and Information Sciences, Radboud University
A Novel Approach to Prevent Session Hijacking Attack


Index Terms

Computer Science Security

Keywords

Session Hijacking, One Time Cookie, Reverse proxy server, Browser fingerprinting, session ID, IP address, Blowfish Algorithm, HTTP