IEEE Access, vol.10, pp.40381-40390, .

HTB: a very effective method to protect web servers against BREACH attack to HTTPS

R. Palacios Hielscher; A. Fariña Fernández-Portillo; E.F. Sánchez Úbeda; P. F. García de Zúñiga Hernández

Abstract-

BREACH is a side-channel attack to HTTPS that allows an attacker to obtain victims&rsquo; credentials under certain conditions. An attacker with a privileged position on the network can guess character by character a secret session key just by analyzing the size of the responses returned by the server over HTTPS and encrypted. Heal the Breach (HTB) is the proposed technique to mitigate BREACH attack by randomly changing the size of server responses through a modified gzip library. The attacker needs a precision of one byte in the size of the responses to be able to determine if a guess character is part of the secret token. Since the modified gzip library introduces randomness in the size of the response, BREACH becomes ineffective. The only way to circumvent this protection is to make several requests and compute the average size of the response, which minimizes the random effect. Mathematical and experimental results show that, for a random variation of the size from 1 to 10 bytes, an attacker needs to analyze 500 times more packages to obtain enough accuracy and surpass this mitigation. However, if the number of requests increases it is easier to isolate and block the attack using standard Intrusion Detection Systems (IDS). Compared to other mitigations, the approach presented in this paper is very effective, easy to implement for all websites hosted in the server, and produces a negligible increase in normal traffic.

Index Terms- BREACH, CRIME, gzip library, HTTPs, side-channel attacks.

Citation:
Palacios, R.; Fariña Fernández-Portillo, A.; Sánchez-Úbeda, E.F.; García-de-Zúñiga, P. "HTB: a very effective method to protect web servers against BREACH attack to HTTPS", IEEE Access, vol.10, pp.40381-40390, .