Abstract

In Cyber security, Denial-of-service (DoS) and distributed DoS (DDoS) are two major threats, and client puzzle, which demands a consumer to perform computationally dear operations before being granted services from a server, is a well-known countermeasure to them. However, a wrongdoer will inflate its capability of DoS/DDoS attacks with quick puzzle solving package and/or intrinsic graphics process unit (GPU) hardware to considerably weaken the effectiveness of consumer puzzles. This paper shows how to stop DoS/DDoS attackers from inflating their puzzle-solving capabilities. To this end, this paper introduces a new consumer puzzle said as software puzzle. Unlike the existing consumer puzzle schemes, which publish their puzzle algorithms in advance, a puzzle algorithmic program in the gift package puzzle theme is at random generated solely once a consumer request is received at the server aspect and therefore the algorithm is generated specified: 1) Associate in Nursing wrongdoer is unable to arrange Associate in Nursing implementation to unravel the puzzle before and 2) the wrongdoer wants extended effort in translating a central process unit puzzle package to its functionally equivalent GPU version such that the interpretation can't be drained real time.
Moreover, the paper shows how to implement package puzzle within the generic server-browser model.

References

17. B. Barak et al., “On the (Im)possibility of obfuscating programs,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2139. Berlin, Germany: Springer-Verlag,
2001, pp. 1–18.


Index Terms

Computer Science

Software Engineering

Keywords

Software puzzle, Code Obfuscation, GPU programming, Denial of Service (DoS), Distributed Denial of Service (DDoS)