Improving security performance with parallel crypto operations in SSL bulk data transfer

ABSTRACT

Information security, including integrity and privacy, is an important concern among todayôs computer users due to increased connectivity. Despite a number of secure algorithms that have been proposed, the trade-offs made between security and performance demands further research toward improvement. For example, in bulk data transfer, especially in large messages, the secured processing time takes much longer than non-secured processes. This is due to crypto operations, which include symmetric encryption operations and hashing functions. In the current bulk data transfer phase in Secure Socket Layer (SSL), the server or the client firstly calculates the Message Authentication Code (MAC) of the data using HMAC operation, and then performs the symmetric encryption on the data together with the MAC. This paper proposes a new algorithm which provides a significant performance gain in bulk data transfer without compromising the security. The proposed algorithm performs the encryption of the data and the calculation of the MAC in parallel. The server calculates the MAC of the data at the same time as the encryption process of the data. Once the calculation of the MAC is completed, only then the MAC will be encrypted. The algorithm was simulated in two processors with one processor performing the MAC calculation and the other on encrypting the data, simultaneously. The communication between the two processors was done via Message Passing Interface (MPI). Based on the performance simulations, the new parallel algorithm gained speedup of 1.74 with 85% efficiency over the sequential (current) algorithm.

Keyword: Information security; Bulk data transfer; Parallel crypto operations; Hashing; Encryption