The attack trace found by OFMC shows that the communication between A and B in this protocol is intercepted by an intruder who impersonates B, thus, performing a man in the middle attack. Therefore, A uses the public key of the intruder to encrypt its identity, intruder's identity, number of request, and a symmetric key known to A. This encrypted information is sent to the intruder who, upon decrypting, makes a few changes such as excluding itself from the message and adds B's identity instead and creates a new request number and a symmetric key and forwards it to B (a web server), encrypting it using B's public key. This step shows that B will presume that the message was sent from A since it includes A's identity. Furthermore, the protocol requires A to authenticate itself to B using a trusted third party s with whom A shares a secret password. Thus, using the symmetric key sent by the intruder, B encrypts the identities of A, itself, s, and a request ID and sends it to the intruder. The intruder forwards this message to A but replaces the identity of B and the request ID with its ID and a forged request ID and encrypts it using the symmetric key sent by A earlier. The subsequent steps in the protocol requires A to communicate with s so that the latter can authenticate the former to B. These transmissions are again intercepted by the intruder who first forwards the message from A to s and then instead of s forwarding the message to B, sends it to the intruder and encrypts it using the public key of B. Upon decrypting, B can verify the message with the assumption that it is indeed sent from s since the identity of s and A are encrypted using the private key of s (this is also a step in the protocol). In conclusion, B presumes that the intruder is A and, hence, sends confidential data/information to the intruder.