World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:11, No:04, 2017

An Aspiring Solution to the Man in the Middle Bootstrap Vulnerability

Authors : Mouad Zouina, Benaceur Outtaj

Abstract : The proposed work falls within the context of improving data security for m-commerce systems. In this context we have placed under the light some flaws encountered in HTTPS the most used m-commerce protocol, particularly the man in the middle attack, shortly MITM. The man in the middle attack is an active listening attack. The idea of this attack is to target the handshake phase of the HTTPS protocol which is the transition from a non-secure connection to a secure connection in our case HTTP to HTTPS. This paper proposes a solution to fix those flaws based on the upgrade of HSTS standard handshake sequence using the DNSSEC standard.

Keywords : m-commerce, HTTPS, HSTS, DNSSEC, MITM bootstrap vulnerability
Conference Title : ICCISSP 2017 : International Conference on Computing, Information Systems Security and Privacy
Conference Location : Zurich, Switzerland
Conference Dates : April 20-21, 2017