RESEARCH ARTICLE

An Enhanced Authentication Scheme Using Kerberos with Hash-Based Message Authentication Code (HMAC)

R. Kogila

Department of Computer Science, Periyar University, TamilNadu, India

kogimca@gmail.com

Abstract— In this thesis, present a new secure authentication system is proposed that significantly reduces the possibility of frauds. This scheme is primarily designed for organizations. It is based on the Kerberos cryptographic framework that has been proven to be secure after being used in real world for decades. The proposed system allows tokens to be exchanged between the server and clients. The token is generated from the client information. A token is cryptographically secure and valid only for the designated client, and therefore it is robust against eavesdropping. The token is compared of Hash Message Authentication Code (HMAC) patent. It is symmetric key cryptography used to describe the underlying cryptographic schemes, the operating principles, and the system design. The proposed system provides authentication, for a more secure protection against the middle attacks. Also increased the timestamp since transports such as Remote Procedure Call (RPC) and Hypertext Transfer Protocol (HTTP) rely on the maximum token size. Show the authentication of system, and discuss the performance.

Full Text: http://www.ijcsmc.com/docs/papers/July2013/V2I7201374.pdf