Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.162 – 168

RESEARCH ARTICLE

Hierarchical EAP Back-End Authenticator State Machine

Desai Malav[1], Kalpesh Patel[2]
[1]Department of Information Technology, Gujarat Technological University, Ahmedabad, India
[2]Department of Computer Science and Engineering Gujarat Technological University, Ahmedabad, India

[1] 13malav@gmail.com; [2] Kalpeshpatel1@yahoo.com

Abstract— Authentication is a basic requirement for telecommunication network market for allowing resources to the legitimate users. Extended Authentication Protocol (EAP) is a widely used protocol for authentication. EAP is basically a framework which supports several authentication methods. The several authentication methods supported by a single protocol make this protocol a complex one. To simplify this Complexity State Machines are used. Extended Authentication Protocol (EAP) also has the state machines provided by Internet Engineering Task Force (IETF). 1) EAP peer 2) EAP stand-alone authenticator which is non-pass-through 3) EAP backend authenticator which is used for Authentication, Authorization, and Accounting (AAA) servers, and 4) EAP full authenticator which is for both local and pass-through, are four state machines presented by IETF. These states machines are created using basic single level state machine which reduces the complexity of state machine up to some point. In this paper we will see how we can reduce the architectural complexity using Hierarchical State Machine. Here we will try to represent the hierarchical state machine structure and implement it for the Back-end Authenticator State Machine.

Key Terms: - Extended Authentication Protocol; EAP; EAP state machines; EAP peer; Back-end State Machine; Hierarchical Approach

Full Text: http://www.ijcsmc.com/docs/papers/May2013/V2I5201373.pdf