

Management and Agreement Protocol in Computer Security

Authors : Abdulameer K. Hussain

Abstract : When dealing with a cryptographic system we note that there are many activities performed by parties of this cryptographic system and the most prominent of these activities is the process of agreement between the parties involved in the cryptographic system on how to deal and perform the cryptographic system tasks to be more secure, more confident and reliable. The most common agreement among parties is a key agreement and other types of agreements. Despite the fact that there is an attempt from some quarters to find other effective agreement methods but these methods are limited to the traditional agreements. This paper presents different parameters to perform more effectively the task of the agreement, including the key alternative, the agreement on the encryption method used and the agreement to prevent the denial of the services. To manage and achieve these goals, this method proposes the existence of an control and monitoring entity to manage these agreements by collecting different statistical information of the opinions of the authorized parties in the cryptographic system. These statistics help this entity to take the proper decision about the agreement factors. This entity is called Agreement Manager (AM).

Keywords : agreement parameters, key agreement, key exchange, security management

Conference Title : ICCSIT 2015 : International Conference on Computer Science and Information Technology

Conference Location : Paris, France

Conference Dates : January 23-24, 2015