Improving the security of mobile IPV6 signalling using KECCAK / SHA-3

ABSTRACT

Most people nowadays use their mobile devices to stay connected to the internet all over the place and all the time. In order to provide their customers with excellent service, all Internet Service Provider (ISP) worked together to make a handover process from one ISP to another. The signalling process is an integral part of the handover that makes it easier for devices to register their new address. If no security is used, attackers could initiate an adverse action during the signalling time. The Mobile IPv6 standard mandates the use of Internet Protocol Security (IPsec) to secure the handover process, particularly during the signalling step. The conventional IPsec uses Keyed-Hash Message Authentication Code-Secure Hash Algorithm-1 (HMAC-SHA-1) to authenticate signalling messages. However, the SHA-1 has been detected and broken by collision attacks and length-extension attacks. Hence, the signalling process on the Mobile IPv6 is vulnerable. The aim of this paper is to find a hash algorithm that is resistant to both attacks. Subsequently, it can be implemented on IPsec to secure the Mobile IPv6 signalling process. The experimental result showed that the SHA-3 algorithm could fulfil the requirements. It can enhance security performance and, at the same time, does not lengthen the authentication time significantly.