World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:06, 2020

Generation of Symmetric Key Using Randomness of Hash Function

Authors : Sai Charan Kamana, Harsha Vardhan Nakkina, B.R. Chandavarkar

Abstract : In a highly secure and robust key generation process, a key role is played by randomness and random numbers when current real-world cryptosystems are observed. Most of the present-day cryptographic protocols depend upon the Random Number Generators (RNG), Pseudo-Random Number Generator (PRNG). These protocols often use noisy channels such as Disk seek time, CPU temperature, Mouse pointer movement, Fan noise to obtain true random values. Despite being cost-effective, these noisy channels may need additional hardware devices to continuously communicate with them. On the other hand, Hash functions are Pseudo-Random (because of their requirements). So, they are a good replacement for these noisy channels and have low hardware requirements. This paper discusses, some of the key generation methodologies, and their drawbacks. This paper explains how hash functions can be used in key generation, how to combine Key Derivation Functions with hash functions.

Keywords : key derivation, hash based key derivation, password based key derivation, symmetric key derivation
Conference Title : ICCALDO 2020 : International Conference on Computer Architecture, Logic Design and Organization
Conference Location : Venice, Italy
Conference Dates : June 22-23, 2020