World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:10, No:12, 2016

Proactive WPA/WPA2 Security Using DD-WRT Firmware

Authors : Mustafa Kamoona, Mohamed El-Sharkawy

Abstract : Although the latest Wireless Local Area Network technology Wi-Fi 802.11i standard addresses many of the security weaknesses of the antecedent Wired Equivalent Privacy (WEP) protocol, there are still scenarios where the network security are still vulnerable. The first security model that 802.11i offers is the Personal model which is very cheap and simple to install and maintain, yet it uses a Pre Shared Key (PSK) and thus has a low to medium security level. The second model that 802.11i provide is the Enterprise model which is highly secured but much more expensive and difficult to install/maintain and requires the installation and maintenance of an authentication server that will handle the authentication and key management for the wireless network. A central issue with the personal model is that the PSK needs to be shared with all the devices that are connected to the specific Wi-Fi network. This pre-shared key, unless changed regularly, can be cracked using offline dictionary attacks within a matter of hours. The key is burdensome to change in all the connected devices manually unless there is some kind of algorithm that coordinate this PSK update. The key idea of this paper is to propose a new algorithm that proactively and effectively coordinates the pre-shared key generation, management, and distribution in the cheap WPA/WPA2 personal security model using only a DD-WRT router.

Keywords : Wi-Fi, WPS, TLS, DD-WRT
Conference Title : ICWWIC 2016 : International Conference on Wired/Wireless Internet Communications
Conference Location : Bangkok, Thailand
Conference Dates : December 12-13, 2016