

EMERGING SECURITY TRENDS AND CHALLENGES IN NETWORK

ASTHA PAREEK¹ & MANISH GUPTA²

¹ICG, Jaipur Rajasthan, India

²Dy. Director (IT), RCEE, Deptt. of Education, GoR, India

ABSTRACT

Wireless networking has been enjoying fast development, evidenced by wide deployments of many wireless networks of various sizes, such as wireless personal area networks (WPANs), local area networks (WLANs), metropolitan area networks (WMANs), and wide area networks (WWANs). The rapid growth and deployment of wireless systems into a wide range of networks and for a wide variety of applications drives the need to support security solutions that meet the requirements of a wide variety of customers. Wireless security can be broken into two parts: Authentication and encryption. Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa, while encryption mechanisms ensure that it is not possible to intercept and decode data. A wireless LAN is a flexible data communication system using electromagnetic waves for transmission and reception of data over the air. In a typical WLAN configuration, a transmitter/receiver device known as access point connects to the wired network using Ethernet cable. The IEEE 802.11 standard specifies optional security called "Wired Equivalent Privacy" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. This paper discusses traditional security methods and challenges.

KEYWORDS: Wireless Network, IEEE 802.11, Wired Equivalent Privacy