Abstract

Network Security is a major issue in wired and wireless network. Wireless Network is more vulnerable to attack. Vulnerability is the threat to the network in the form of virus or the way used by attacker in order to breach the security and bypass the security measures. IEEE 802.11i and 802.11-2007 provides RSNA methods for wireless network security. WECA, the alliance for Wi-Fi devices provides WPA2 modes of security. The responsibility of network administer is to provide network resources to the legitimate and authorized users and at the same is to protect it from illegitimate and misuse by unauthorized, immoral unlawful clients and cyber criminals and also to find the solution for the other security threats such as Phishing, malware and malicious code. The Network resources are made available by way of authentication and authorization of users. The protection against illegal and misuse of network is taken place by applying some RSNA and WPA2 Methods. But these authentications, authorizations and protections of RSNA and WPA2 modes are weak and vulnerable to numerous attacks and its advanced version such as 802.11n with AES gets compatibility issues with software as well as with hardware. This Paper, by developing a practical network scenario and configuring its devices according to various RSNA and WPA2 modes examines
these security measures and conclude that these security methods are not sufficient and requires more other measures. These others measures such as web browser compatibilities, OS effectiveness, firewall and hardware security modules have been taken into account in order to develop a secure wireless Network Model. Various Network Monitoring tools have also been used to show that how easily the security is breached and/or bypassed.

References

- Shivaputtrappa Vibhuti, &quot;IEEE 802. 11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability&quot; , San Jose State University, CA, USA, CS265 Spring 2005 (26.03.2005)
- Lu Zhengqiu; Tian Si; Wang Ming; Ye Peisong; Chen Qingzhang; &quot;Security analysis and recommendations for Wireless LAN 802. 11b network&quot;, Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on 16-18 April 2011.
- Finn Michael Halvorsen & Olav Haugen &quot;Cryptanalysis of IEEE 802. 11i TKIP&quot;, Norwegian University of Science and Technology, June 2009.
- Back and Tews &quot;Practical attacks against WEP and WPA&quot;, November 8, 2008.
- Paul Arana, &quot;Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)&quot;, INFS 612 – Fall 2006.
- A. K. M. Nazmus Sakib et al &quot;Security Improvement of WPA 2 (Wi-Fi Protected Access 2)&quot; (IJEST), Vol. 3 No. 1 Jan 2011
- Vijay Chandramouli, &quot;A Detailed Study on Wireless LAN Technologies&quot;, 23. 10. 2002
- Understanding the New WPA TKIP Attack Vulnerabilities & Motorola WLAN
Countermeasures”, Motorola, Inc. 2008.
- Dajiang He, Charles. Q. Shen. “Simulation study of IEEE 802.11e EDCF”;
  2003
- Ismahnsi Binti Ismail, “Study of Enhanced DCF(EDCF) in Multimedia
  Application”; 2005
- Preeti Venkateswaran, “Experiments to Develop Configurable Protocols”;
  2005
- Mark Greis, Tutorial for the Network Simulator “ns”; 2008
- Lecture notes 2003-2004 University de Los Andes, Merida, Venezuela and ESSI
  Sophia-Antipols, France.
- Guillermo Alonso Pequeño Javier Rocha Rivera, “Extension to MAC 802.11 for
  performance improvement in MANET”; 2007
- Sam De Silva, Using TCP “Effectively in Mobile Ad-hoc Wireless Networks with
  Rate Adaptation”; 2007
- Turkam Ahamad & Manar Younis “The Enhancement of Routing Security in Mobile
  Ad-hoc Networks”; IJCA(0975 – 888), Volume 48– No. 16, June 2012.
- Payal Pahwa, Gaurav Tiwari, Rashmi Chhabra “Spoofing Media Access Control
  (MAC) and its Counter Measures”; IJAEA, Jan. 2010.
- Farhad Soleimanian & Zeinab Abbasi “Analysis and Evaluation of Dynamic Load
  Balancing in IEEE 802.11b Wireless Local Area”; IJCA(0975 – 888), Volume 47– No. 22,
  June 2012.
- Fanglu Guo and Tzi-cker Chiueh “Sequence Number-Based MAC Address Spoof
  Detection”; 2005.
- Stuart Compton, SANS Institute, “802.11 Denial of Service Attacks and
- D. Gupta, G. Tiwari,Y. K and P. Kumar “Media Access Control (MAC) MAC
  Spoofing and its Counter Measure”; IJRTE, 2009
- Siemens Enterprise Communications, “WLAN Security Today: Wireless more
  Secure than Wired”; white paper July 2008.
- Website :http://milesweb. com , Aug 2012
- Website : http://www. technitium. com, Aug 2012
- Website : http://www. klconsulting. net/smack.
- Website: http://www. softpedia. com/ get/ Network-Tools/ IP-Tools/ IPScan-II. shtml
- Website : http://ip-scan. qarchive. org/, May 2012
- Website : ww. radmin. com/products/ipscanner, May 2012
- Website : http://www. angryip. org/w/Home, May 2012
- Website : http://www. opnet. com/itguru-academic
- Website : http://www. makeuseof. com
- Website :http:// Cisco. com aug 2012
- Richa Bansal, Siddharth Tiwari, Divya Bansal “Non-cryptographic methods of MAC

**Index Terms**

- Computer Science
- Security

**Keywords**

- WLAN
- CSMA/CA
- CCMP
- TKIP and MAC