**LM 4. Wireless Network Threats & Vulnerabilities**

1. **LM4. Student Learning Outcomes**

After completing this module, a student will be able to:

* Describe different types of attackers
* Describe the vulnerabilities of WLAN in general
* Describe WEP, WPA and WPA2 and their vulnerabilities.
* Explain what’s passive attack and what’s active attack. List two examples of each types attack.
* Describe confidentiality, access control, availability, authentication and integrity attacks on WLAN.
* Discuss Bluetooth security features
* Describe Bluetooth vulnerabilities and threats
* Describe the threat models of the Ad Hoc wireless network

1. **LM4. Learning Material & Study Guide**

Note: this module covers vulnerabilities and threats of WLAN, Bluetooth, and Ad Hoc Wireless Network.

* Describe different types of attackers

<https://www.walshcollege.edu/upload/docs/CyberSpring/Profile%20of%20a%20Cyber%20Attacker%20Presentation.pdf>

-page 10 of the slides

* Describe the vulnerabilities of WLAN in general

<https://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf>

-section IV. What’s the characteristics of WLAN make it vulnerable; security protocols used in WLAN, MAC address filtering, and default SSID & password.

* Describe WEP, WPA and WPA2 and their vulnerabilities.

<http://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2>

<https://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf>

-section IV.

* Explain what’s passive attack and what’s active attack. List two examples of each types attack.

<https://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf>

-section V.

* Describe confidentiality, access control, availability, authentication and integrity attacks on WLAN.

<https://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf> pages 179 -181.

* Discuss Bluetooth security features

<https://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/wireless-computing/sec_bluetooth.shtml>

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf> page 10 and 11. The security modes of Blue tooth.

* Describe Bluetooth vulnerabilities and threats

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf> page 25-28.

* Describe the threat models of the Ad Hoc wireless network

<https://www.utc.edu/center-information-security-assurance/pdfs/course-paper-5620-ad-hoc-security.pdf> Section 2 and 3.