VULNERABILITIES OF WIRELESS NETWORKS AND EXISTING THREATS

L.E. Bulygin, P.V. Gunov, M.E. Semenov

National Research Tomsk Polytechnic University,

Russia, Tomsk, Lenina Avenue, 30, 634050

E-mail: leb1@tpu.ru

Wireless technologies have received the massive development and have become part of business and everyday life. On basis of these technologies can create Internet access points and wireless local area networks (WLAN). Currently WLAN are wide used in most companies, enterprises scientific centers, and universities. Information is strategic assets of organizations, and network malfunctions, data interception can lead to negative consequences: loss of time, money, and reputation... Therefore, the security of WLAN is an actual problem.

Objective of research is to review of existing methods for ensuring security for wireless networks, their weaknesses and threats. To achieve the objective need to complete the following tasks: review of existing methods of wireless security networks, review of their vulnerabilities and identify existing threats.

WLAN operates according to the standard IEEE 802.11 (Institute of Electrical and Electronics Engineers), which is created for communication in a wireless local area. To protect against attackers in the standard IEEE 802.11 protocol provides a range of security measures: for example, authentication, encryption of traffic, MAC-address filtering and restricting access.

Wireless networks can be protected by the following technologies: open mode (not used any encryption or authentication), WEP (Wired Equivalent Privacy) and WPA/WPA2 (Wi-Fi Protected Access). An overview of WLAN security technologies is presented in Table 1.

Table 1. Overview of WLAN security technologies

Mode	Attack techniques	Elapsed time	Computing resources	Places of use networks
WEP	Exhaustive key search, social engineering, unauthorized access to equipment	From several minutes to several hours	A personal computer	Public places, residential space, business space
WPA/ WPA2	Exhaustive key search, encryption exploits, social engineering, unauthorized access to equipment	From several hours to several days	A personal computer, a supercomputer	Residential space, business space

Despite the use of different security methods there are serious threats of the use of wireless networks. The method of hacking the WPA key for 12-15 minutes was demonstrated [1]. This method was improved [2] and as a result, the execution time of proposed attack method becomes about one minute.

Practical recommendations how to protect wireless networks and reduce the risk of data interception will be presented in our oral report.

REFERENCES

1. Tews E. Gone in 900 Seconds, Some Crypto Issues with WPA, PacSec 2008 Conference, Nov. 2008, Tokyo, Japan.
2. Ohigashi T., Morii M. A Practical Message Falsification Attack on WPA, Hiroshima, Japan, 2009.