WI-FI NETWORKS: PENETRATION AND PROTECTION

A. Kuchko
VSU named after P.M. Masherov, Vitebsk, Belarus

Access to the Internet can be obtained almost anywhere. In the park, in a cafe, at school, at the university and at public transport stops. This is made possible by wireless access networks. We are used to refer to such wifi networks, but this is only a trademark, so do not talk about it. In connection with the spread of this technology, it is likely that your traffic will be able to track. To secure users, wireless security protocols were developed: WEP, WPA/WPA2, WPS, OPEN.

The purpose of this work is find vulnerabilities in wireless network security protocols, to study them and make recommendations for security.

Material and methods. To compare the security protocols, we used data on the vulnerabilities of these protocols**.** The messages of different users on the forums in the Internet were analyzed. Documentation for wireless network security protocols was studied.

Results and their discussion. OPEN is the absence of any protection. The access point and the client do not mask the data transmission in any way. Almost any wireless adapter in any laptop with Linux can be installed in the listening mode, when instead of discarding packets intended not for him, it will capture them and transfer them to the OS where they can be easily viewed.

It is on this principle that wired networks operate - they do not have built-in protection and “crashing” into it or simply connecting to a hub / switch, the network adapter will receive packets of all devices in this network segment in an open form. However, with a wireless network, you can “crash” from anywhere – 10–20–50 meters and more, and the distance depends not only on the power of your transmitter, but also on the length of the hacker's antenna. Therefore, open data transmission over a wireless network is much more dangerous.

WEP is the first standard for Wi-Fi protection. It stands for Wired Equivalent Privacy, but in fact it gives much less protection than these wired networks, because it has a lot of flaws and is hacked in many different ways, which, due to the distance covered by the transmitter, makes the data are more vulnerable. It should be avoided almost as much as open networks - it provides security only for a short time, after which any transmission can be completely opened regardless of the complexity of the password. The situation is aggravated by the fact that passwords in WEP are either 40 or 104 bits, which is an extremely short combination and it can be picked up in seconds (this is without taking into account the errors in the encryption itself).

WEP was invented in the late 90's, which justifies it, but those who still use it – no.

The main problem of WEP is in the fundamental design error. Stream encryption is done using a temporary key. WEP actually transmits several bytes of this key together with each data packet. Thus, regardless of the complexity of the key, you can open any transfer simply by having a sufficient number of intercepted packets (several tens of thousands, which is quite small for an actively used network).

WPA is the second generation that replaced WEP. It stands for Wi-Fi Protected Access. A qualitatively different level of protection due to the consideration of WEP errors. The password length is arbitrary, from 8 to 63 bytes, which greatly complicates its selection (compare with 3, 6 and 15 bytes in WEP).

The standard supports various encryption algorithms for the transmitted data after the handshake: TKIP and CCMP. The first is a kind of bridge between WEP and WPA, which was invented at that time, while IEEE was busy creating a full-fledged CCMP algorithm. TKIP, like WEP, suffers from some types of attacks, and is generally not secure. Now it is rarely used and in general, the use of WPA with TKIP is almost the same as using a simple WEP.

One of the fun features of TKIP is the possibility of a so-called Michael attack. To quickly patch up some particularly critical holes in WEP in TKIP, it was introduced the rule that the access point should block all communications through itself (that is, "fall asleep") for 60 seconds if an attack is found on the key selection. Michael-attack - a simple transfer of "corrupted" packages to completely disconnect the entire network.

In addition to different encryption algorithms, WPA / WPA2 supports two different initial authentication modes (password checks for client access to the network) - PSK and Enterprise. PSK (sometimes referred to as WPA Personal) is an input by a single password that the client enters when connected. It's simple and convenient, but in the case of large companies it can be a problem - say, your employee left and that he could no longer access the network have to change the password for the entire network and notify other employees about it. Enterprise removes this problem due to the presence of multiple keys stored on a separate server - RADIUS. In addition, Enterprise standardizes the authentication process itself in the EAP (Extensible Authentication Protocol) protocol, which allows you to write your own algorithm.

WPS is an interesting technology that allows us not to think about the password at all, but simply to press the button and immediately connect to the network. In fact, this is a "legal" method of bypassing password protection in general, but surprisingly, it was widely distributed with a very serious miscalculation in the access system itself - it's years after the sad experience with WEP.

WPS allows the client to connect to the access point using the 8-character code consisting of digits (PIN). However, due to an error in the standard, only 4 of them need to be guessed. Thus, just 10,000 retry attempts, and regardless of the complexity of the password for accessing the wireless network, you automatically get this access, and with it, in addition - and this same password as it is.

Given that this interaction occurs before any security checks, you can send 10–50 requests to the WPS throughput per second, and after 3–15 hours (sometimes more, sometimes less) you will receive the keys. When this vulnerability was revealed, manufacturers began to introduce a limit on the number of login attempts (the rate limit), after exceeding which the access point automatically for some time disables the WPS - but so far such devices are not more than half of those already released without this protection. Even more - a temporary shutdown cardinally does not change anything, since at one login attempt per minute we will need only 10000/60/24 = 6.94 days. And the PIN is usually found before the whole cycle goes through. I want to draw your attention once again that with WPS enabled, your password will be inevitably disclosed, regardless of its complexity. Therefore, if you generally need WPS - turn it on only when connecting to the network, and at other times keep this backdoor turned off.

Conclusion. The research revealed vulnerabilities in all security protocols. This shows that using wifi networks is not safe. Wifi is not suitable for transferring secret information. In order to maximize your safety, follow these simple recommendations: do not connect to open networks, before connecting, check the protocol type, use the latest version of the software.

Reference list:

1. Ross, J. Wi-Fi, wireless access networks, 2005. – 98 p.
2. Olifer, F. Computer networks. Principles, technologies, protocols, 2016. – 72 p.
3. Sergeev, A. Fundamentals of local computer networks, 2013. – 205 p.
4. Odom, U. Routing and Switching, 2016. – 103 p.
5. Chaika, U. Modern wireless networks, 2011. – 202 p.

ON THE PROPERTIES OF FITTING CLASSES, GENERATED π-CORADICALS

K. Lantsetova

VSU named after P.M. Masherov, Vitebsk, Belarus

Only finite groups are considered. In the definitions and notation we follow [1].

A class $\mathfrak{F}$ is a *Fitting class* if and only if the following two conditions are satisfied: