Elmi Xəbərlər Jurnalı *Nömrə 2, 2025* 16-19

DOI:10.30546/gdu.2.2025

WPS PROTOKOLUNUN TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Quliyev Anar Rəsul oğlu
Gəncə Dövlət Universiteti
anar.quliyev.1972@mail.ru

Xülasə. *Məqalədə WPS protokolunun müdafiəsində qarşıya çıxan bəzi zəifliklər müzakirə olunur. Bəzən simsiz şəbəkəyə kobud güc hücumu baş verir. Araşdırma zamanı variasiyaların sayını azaltmaq imkanları, kobud güc hücumlarının qarşısının alınması üçün PIN kodlardan istifadə imkanları öz əksini tapır.*

Açar sözlər: simsiz şəbəkələr, nöqtə giriş, zəiflik, təhlükəsizlik.
Ключевые слова: беспроводные сети, точка доступа, уязвимость, безопасность.
Keywords: wireless network, access point, vulnerability, security.

Müasir simsiz məlumat ötürmə texnologiyaları həm böyük şirkətlərin istehsal fəaliyyətlərində, həm də kompüter şəbəkələrinin qurulmasında geniş istifadə olunur, Simsiz WiFi şəbəkəsi baza stansiyaları - giriş nöqtələri əsasında qurulur. Müasir giriş nöqtəsinin əhatə dairəsi təxminən 100 m-dir. Eyni zamanda, bir nöqtə eyni vaxtda bir neçə onlarla aktiv istifadəçini dəstəkləyə bilir və 400 Mbit/s-ə qədər məlumat ötürmə sürətini təmin edir.Bu zaman simsiz şəbəkələrin təhlükəsizliyinə çox diqqət yetirilir. IEEE 802.11 simsiz şəbəkə spesifikasiyası təhlükəsizlik protokolunu müəyyən edir.

WEP (Wired Equivalent Privacy) RC4 alqoritmi əsasında ötürülən məlumat axınını 64 və ya 128 bit açar ölçüsü ilə şifrələməyə imkan verir. Bununla belə, bu protokolda fundamental boşluqlar aşkar edilib ki, bunun nəticəsində təcavüzkar şəbəkə üzərindən ötürülən məlumatları təhlil edərək açarı təxmin edə bilir. Yaranan açar, təcavüzkarın qanuni istifadəçi adı altında şəbəkəyə qoşulmasına imkan verir.

2003-cü ildə təkmilləşdirilmiş simsiz şəbəkə təhlükəsizliyi standartı- WPA (WiFi Protected Access) hazırlanmışdır. Kiçik simsiz şəbəkələr adətən paylaşılan açarlara WPA-PSK (Öncədən Paylaşılan Açar) əsaslanan WPA təhlükəsizlik protokolunun variantından istifadə edirlər. WPA-PSK istifadə edərkən giriş nöqtəsi parametrlərində və müştəri simsiz əlaqə profillərində 8-63 simvoldan ibarət parol göstərilir. 2005-ci ildə WPA2 protokolunun yeni versiyası təqdim edildi.

Kifayət qədər etibarlı şifrələmə alqoritmləri ilə birlikdə müxtəlif EAP (Genişləndirilən Doğrulama Protokolu) autentifikasiya protokollarına dəstək verir:

AES (RC4 əvəzinə) və TKIP (Temporal Key Integrity Protocol).

1. WPS Protokoluna İcmal

Yeni cihazı təhlükəsiz WiFi şəbəkəsinə qoşmaq üçün istifadəçi şəbəkə adını (SSID), parolu və təhlükəsiz simsiz əlaqə parametrlərini əl ilə göstərməlidir. Bu proseduru sadələşdirmək üçün WiFi Alliance 2009-cu ildə WPS (WiFi Protected Setup) protokolunu işləyib hazırladı. WPS protokolundan istifadə edərkən cihazı təhlükəsiz şəbəkəyə qoşmaq üçün xüsusi düyməni sıxmaq kifayətdir. Giriş nöqtəsi və ya PIN kodu daxil edilir. Bu, çox rahatdır, buna görə də bütün əsas şəbəkə avadanlığı istehsalçıları (Cisco/Linksys, Netgear, D-Link, Belkin, TP-Link, ZyXEL) WPS dəstəyi ilə simsiz marşrutlaşdırıcılar istehsal edirlər.

WPS funksiyasından istifadə etmək üçün müxtəlif variantlar var, məsələn:

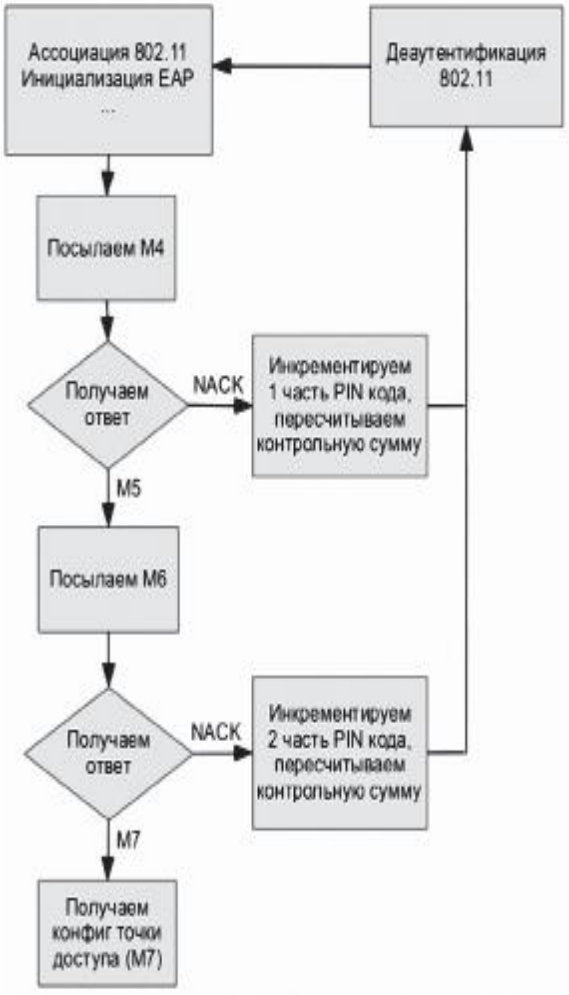
- düyməni sıxmaq – istifadəçi giriş nöqtəsində və qoşulmuş cihazda xüsusi düyməni sıxır və bununla da quraşdırma prosesini aktivləşdirir;
- giriş nöqtəsində PİN kodun daxil edilməsi - marşrutlaşdırıcıya qoşulduqda, PİN kodu düzgün daxil etdiyiniz təqdirdə şəbəkə parametrlərini ala biləcəyiniz xüsusi WPS ilə açа bilərsiniz.

DOI:10.30546/gdu.2.2025

PİN kod 8 rəqəmdən ibarət olduğundan, axtarış üçün cəmi 108 (100 milyon) mümkün variant var. Bununla belə, PİN-in son rəqəmi yoxlama qiymətidir və ilk 7 rəqəm əsasında GTIN-8 alqoritmi ilə hesablanır və bu, mümkün variantların sayını 107-yə (10 milyon) qədər azaldır.

2. WPS protokolunda zəiflik

2011-ci ildə ABŞ Kompüter Fövqəladə Hallara Hazırlıq Qrupu Wi-Fi şəbəkələrini qorumaq üçün simsiz cihazların qoşulmasını sadələşdirmək üçün nəzərdə tutulmuş WPS protokolunda zəifliyi təsvir edən təhlükəsizlik bülleteni nəşr etdi. Zəifliyin mahiyyəti yeni simsiz cihazı birləşdirən zaman PİN kodun düzgünlüyünü yoxlayan giriş nöqtəsinin həyata keçirilməsindədir. WPS autentifikasiya protokolunda PİN-in yoxlanılması iki mərhələdə aparılır: birincisi, 4 rəqəmdən ibarət iki hissəyə bölünür, sonra isə hər bir hissə ayrıca yoxlanılır. Müştəri səhv PİN daxil edibsə, giriş nöqtəsi kodun hansı hissəsini dəqiq müəyyən etmək üçün istifadə oluna bilən EAP-NACK xidmət mesajı göndərir (şək. 1).



1.Əgər M4 paketini göndərdikdən sonra müştəri cavab olaraq EAP-NACK mesajı alırsa, o zaman PİN kodun birinci hissəsinin səhv olduğuna əmin olmaq olar.

2. M6 paketi göndərildikdən sonra EAP-NACK mesajı alınarsa, PİN kodun ikinci hissəsi müvafiq olaraq yanlışdır.

WPS protokolunun bu "xüsusiyyəti" kobud güc hücumu zamanı cəhdlərin sayını əhəmiyyətli dərəcədə azalda bilər. Ümumilikdə birinci üçün 104 (10.000) və ikinci üçün 103 (1000)variant var. Nəticədə məlum olur ki, təcavüzkar yalnız 11.000 variantı sınamalı olacaq.

3. Reaver yardım proqramının istifadəsi WPS protokoluna kobud güc hücumunu həyata keçirmək üçün Tactical Network Solutions tərəfindən hazırlanmış

Reaver yardım proqramından istifadə edilə bilər. O, yalnız WPS-PIN-in seçilməsi və PSK açarının əldə edilməsi Şəkil 1.WPS protokolunun alqoritmi prosesini avtomatlaş dırmır, həm də müxtəlif marşrutlaşdırıcı modellərə qarşı çoxlu sayda hücumun həyata keçirilməsinin qarşısını alır.

Simsiz şəbəkənin təhlükəsizliyini təhlil etmək üçün WPS protoko-da istifadə alqoritmini nəzərdən keçirək:

1)airmon-ng yardım proqramından istifadə edərək simsiz adapteri monitorinq rejiminə qoyun;

2) yuma yardım proqramından istifadə edərək WPS funksiyasının aktivləşdirildiyi giriş nöqtələrinin (BSSID) MAC ünvanlarını əldə edin;

3) Reaver yardım proqramından istifadə edərək bütün mümkün PİN kodlardan keçin.

DOI:10.30546/gdu.2.2025

Reaver yardım proqramı yalnız Linux əməliyyat sistemlərində istifadə edilə bilər, çünki o, simsiz şəbəkə adapterinin işləməsi üçün monitorinq rejimində olmasını tələb edir. Wlan0 simsiz interfeysini monitorinq rejiminə keçirmək üçün əmrdən istifadə edin:

$airmon-ng start wlan0

Reaver yardım proqramının sürəti marşrutlaşdırıcının WPS sorğularını emal etdiyi sürətlə məhdudlaşır. Hər bir PİN kodu yoxlamaq üçün vaxt 3 saniyədirsə, bütün 11.000 variantdan keçmək 10 saatdan çox olmayacaq.

WPS protokolunun sonrakı təhlili göstərdi ki, bəzi marşrutlaşdırıcı modellərinə hücum müddəti əhəmiyyətli dərəcədə azaldıla bilər, çünki aydın mətnlə yayımlanan giriş nöqtəsinin MAC ünvanından PİN kodu hesablamaq mümkündür. Bəzi marşrutlaşdırıcı modellərində PIN kodu birbaşa cihazın özünə yazılır. Sonra, təcavüzkar marşrutlaşdırıcıya fiziki giriş əldə edərsə, qorunan şəbəkəyə qoşulmaq üçün bu koddan istifadə edə bilər.

4. Mühafizə üsulları

Beləliklə, giriş nöqtəsinin əhatə dairəsində olan təcavüzkar, WPS PIN kodunu tapmaq və simsiz şəbəkə üçün parol əldə etmək üçün kobud güc hücumundan istifadə edə bilər. Bundan sonra təcavüzkar marşrutlaşdırıcının parametrlərini dəyişə, müxtəlif növ trafikin qarşısının alınması hücumlarını və giriş nöqtələrinin saxtalaşdırılmasını həyata keçirə bilər. Bu zəiflik ən çox yayılmış WiFi marşrutlaşdırıcılarında mövcuddur, çünki onlar bu hücumun həyata keçirilməsinin qarşısını almırlar. Buna görə də, bu hücum ehtimalını aradan qaldırmaq üçün marşrutlaşdırıcının parametrlərində WPS funksiyasını söndürmək tövsiyə olunur. Lakin bu həmişə mümkün olmur. Məsələn, müvəqqəti istifadə üçün öz müştərilərinə WiFi marşrutlaşdırıcıları təklif edən İnternet provayderləri çox məhdud funksionallıqla dəyişdirilmiş proqram təminatı quraşdırırlar. Buna görə də, istifadəçi hətta WPS funksiyasını söndürmək istəsə belə o, giriş nöqtəsinin özünü dəyişmədən bunu edə bilməyəcək.

WiFi şəbəkəsinin sındırılması ehtimalını azaltmaq mümkün olmadıqda, giriş nöqtəsini söndürmək tövsiyə olunur. Əksər marşrutlaşdırıcılar müəyyən edilmiş vaxtda simsiz şəbəkəni avtomatik yandırmaq-söndürmək üçün konfiqurasiya edilə bilər. Bu funksiya ötürücünün normal istifadə edilmədiyi vaxtlarda onu avtomatik söndürmək üçün konfiqurasiya edilə bilər. Hər bir yad adamın WiFi şəbəkəsinə qoşulmadığından əmin olmaq üçün vaxtaşırı marşrutlaşdırıcının parametrlərində simsiz bağlantılar cədvəlini nəzərdən keçirmək tövsiyə olunur. Eyni zamanda müştərilərin MAC ünvanları haqqında DHCP xidmət qeydlərinə də baxmaqla bunu bilmək olar.

Ədəbiyyat

1. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей. Стандарт IEEE 802.11.М.: РадиоСофт, 2010.
2. Shcherbakov V.B., Ermakov S.A. Wireless network security. IEEE 802.11 standard. M.: RadioSoft,2010.
3. Белорусов Д.И., Корешков М.С. WiFi-сети и угрозы информационной безопасности // Специальная техника. 2009. № 6.
4. Максимов В. Технология Wi-Fi: гарантии безопасности //Компьютер Пресс.2005. №4.
5.Wi-Fi Protected Setup Protocol [Электронный ресурс]. URL: http://en.wikipedia. org/ wiki/Wi-Fi_
6. GTIN-8 Check Digit Calculator [Электронный ресурс]. URL: http://www.gs1.org/barcodes/support/ check_digit_calculator (дата обращения: 20.12.2013).
7. WPS PIN brute force vulnerability // CERT Knowledgebase [Электронный ресурс]. URL: http://

DOI:10.30546/gdu.2.2025

www.kb.cert.org/vuls/id/723755 (дата обращения: (18.12.2013).

ВОПРОСЫ БЕЗОПАСНОСТИ ПРОТОКОЛА WPS

Кулиев Анар Расул оглы

Резюме

В статье рассматривается уязвимость в протоколе WPS, которая позволяет реализовать брутфорс-атаку на беспроводную сеть. Исследованы возможности сокращения количества вариантов PIN-кодов для перебора.

SECURITY ISSUES OF THE WPS PR OTOCOL.

Guliyev Anar Rasul oglu

Summary

The paper discusses the vulnerability of the WPS protocol which leaves a possibility for a brute force attack on the wireless network. The author considers
ways to reduce the number of options for PIN-code for exhaustive key search.

Rəyçi: dos. G.Verdiyeva
İnformatika və cəbr kafedrasının 14 fevral 2025-ci il tarixli 6 saylı protokolu.
Daxil olma tarixi 17 fevral 2025-ci il