УДК 004.65

ОСОБЛИВОСТІ ЗАХИСТУ МЕРЕЖІ WI-FI З ПРОТОКОЛОМ ШИФРУВАННЯ WPA3

Богданов О.С., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності, м. Львів

Проведено дослідження особливостей захисту мережевого трафіку у безпровідникових мережа з використання протоколу WPA, зокрема оновленої версії 3. Висвітлено переваги та недоліки у порівнянні з попередніми версіями.

Ключові слова: WPA3, безпека, шифрування, мережа

A study of the features of network traffic protection in wireless networks using the WPA protocol, in particular the updated version 3. Highlights the advantages and disadvantages compared to previous versions.

Keywords: WPA3, security, encryption, network.

До недавнього часу для надійного захисту мережі Wi-Fi зазвичай було достатньо використовувати WPA2 і досить довге і складне ключове слово. І хоча WPA2 пропонує безліч покращень у плані безпеки в порівнянні з WPA, він все ще страждає від використання слабких паролів. Алгоритм вразливий для атак методом перебору, які можуть бути успішними, коли користувач використовує прості паролі.

Коли клієнт підключається до бездротового пристрою (WiFi-маршрутизатора, точки доступу і т.д.), пароль, який потрібно для підключення, зазвичай передається за допомогою алгоритму WPA2. У 2018 році Wi-Fi Alliance представив WPA3, що відкриває можливості щодо його реалізації для виробників бездротового обладнання зв'язку. WPA і WPA2 з'явилися (перший у 1999 році, а інший – у 2004 році), щоб подолати серйозні недоліки, яким був схильний старий алгоритм WEP.

Крім того, завжди рекомендується не використовувати поширений SSID (ідентифікатор мережі WiFi), оскільки зловмисники можуть використовувати попередньо створені райдужні таблиці для прискорення атаки. Атаки, які використовують PIN-код WPS на маршрутизаторі Wi-Fi для отримання несанкціонованого доступу до мережі Wi-Fi, дуже поширені.

Дослідження Меті Ванхофа вказують на можливість відкриття вмісту пакетів даних, які проходять між захищеними WPA/WPA2 WiFi-маршрутизаторами/точками доступу та клієнтськими пристроями, навіть не зламавши пароль для захисту бездротової мережі інших користувачів. Після оголошення про виявлення вразливості виробники WiFi-пристроїв одразу випустили оновлення програмного забезпечення для виправлення вразливості.

Однак проблема стосується самого стандарту, і оновлення системи безпеки випущені не для всіх пристроїв, що знаходяться в обігу. Тому перехід на нову та безпечнішу версію WPA стає необхідністю, а WPA3, як зазначається у дослідження, забезпечить вирішення усіх недоліків попередньої версії протоколу.

Розробником протоколу шифрування WPA3 є некомерційна асоціація Wi-Fi Alliance, утворена основними «великими» компаніями у галузі IT – Apple, Samsung, Sony, LG, Intel, Dell, Broadcom, Cisco, Qualcomm, Motorola, Microsoft та Texas Instruments).

Усі пристрої Wi-Fi, для яких виробник хоче відобразити логотип Wi-Fi CERTIFIED WPA2 або Wi-Fi CERTIFIED WPA3, повинні суворо відповідати специфікаціям, опублікованим альянсом.

Сьогодні, час при використанні громадських мереж Wi-Fi (наприклад, в аеропортах, готелях, барах та ресторанах, житлових приміщеннях, громадських місцях) їхня безпека залишається «під знаком питання».

Мережний трафік, що генерується пристроєм (за винятком зашифрованого трафіку, наприклад, що передається по HTTPS), після підключення до загальнодоступної мережі Wi-Fi фактично може бути прочитаний третіми особами, підключеними до того ж маршрутизатору або точці доступу. Тому завжди рекомендується використовувати VPN у

таких ситуаціях, що забезпечує найкращі гарантії при використанні загальнодоступного Wi-Fi, керованого третіми особами.

Якщо у є VPN-сервер у домашній або офісній мережі (найповніші та універсальні маршрутизатори підтримують OpenVPN), можливо встановити віддалене зашифроване з'єднання або використовувати службу VPN.

WPA3 дозволяє подолати ці проблеми, активуючи індивідуальне шифрування даних: щоразу, коли абонемент підключається до загальнодоступного Wi-Fi, весь трафік, що передається між окремим пристроєм і точкою доступу, буде зашифрований, навіть якщо пароль не вимагався.

Щоразу, коли пристрій підключається до точки доступу Wi-Fi, запускається процедура, яка називається рукостисканням, яка дозволяє перевірити правильність введеного пароля та продовжити узгодження з'єднання.

Процедура рукостискання виявилася вразливою для атак методом перебору, хоча виправлення, випущені різними виробниками обладнання, дозволяють мінімізувати ризики.

WPA3 встановлює новий спосіб виконання рукостискання, надійний та виключає використання методу «грубою сили». Рішення WPA3 настільки надійне, що робить мережу Wi-Fi захищеною, навіть якщо користувач встановить простий пароль.

За останні кілька років світ сильно змінився, і тепер все частіше трапляються пристрої з інтерфейсом Wi-Fi, які не мають дисплея. Це насамперед пристрої, що належать світові Інтернету речей (IoT).

Для підключення цих пристроїв до мережі Wi-Fi зазвичай потрібно встановити програму або підключитися до локального веб-сервера, встановленого на цих пристроях, за допомогою іншого терміналу, підключеного до тієї ж локальної мережі.

WPA3 включає функцію, яка покликана спростити процес налаштування кожного пристрою Wi-Fi без дисплея.

Високий рівень безпеки для промислових програм. WPA3 включає 192-бітовий пакет безпеки, який зробить використання нового протоколу придатним для всіх додатків, де важлива конфіденційність даних. Такі специфікації дозволять активувати захист військового рівня, який також може використовуватись державними органами та компаніями для промислового застосування.

Слід зазначити, що для кожного WiFi-маршрутизатора WPA3 повинні використовуватися бездротові клієнти, сумісні з WPA3. В іншому випадку нові функції WPA3 не можуть бути використані. З метою легкого переходу клієнтів на новий стандарт, WPA3-сумісні маршрутизатори також зможуть приймати з'єднання WPA2. Крім того, навіть коли WPA3 буде досить поширеним, слід очікувати досить тривалого перехідного періоду, протягом якого деякі пристрої будуть підключатися до маршрутизатора через WPA3, а інші – через WPA2.

Таким чином, на основі проведеного аналізу особливостей реалізації нового протоколу WPA3, можна зробити висновок про необхідність його терміново впровадження в усіх сферах використання безпровідникових мереж різного призначення. Інтеграційні процеси не передбачають одночасної заміни всіх мережевих інтерфейсів та їх програмного забезпечення. Впровадження можливе поступово, оскільки у стандарті WPA3 залишиться підтримки попереднього стандарту WPA2.

Література

1. Що таке WPA3 і як він робить мережі Wi-Fi більш безпечнішими. [Електронний ресурс] – режим доступу до ресурсу - https://windows-school.ru/blog/chto_takoe_wpa3/2020-05-24-641.
2. Протокол WPA3: нове покоління чи планова модернізація WiFi? [Електронний ресурс] – режим доступу до ресурсу - https://wifi-solutions.ru/protokol-wpa3-novoe-pokolenie-ili-planovaya-modernizaciya-wifi/
3. Безпека WPA3 [Електронний ресурс] – режим доступу до ресурсу - https://spy-soft.net/wpa3
4. WPA3 – новий рівень безпеки WiFi 802.11. [Електронний ресурс] – режим доступу до ресурсу - https://www.atraining.ru/wpa3-802-11-2018/