АНАЛІЗ БЕЗПЕКИ ІНТЕРФЕЙСУ 802.11(WI-FI З'ЄДНАНЬ), КЛАСИФІКАЦІЯ ПАРОЛІВ

УДК 004.056.5

БОСКІН Олег Осипович
старший викладач кафедри інформаційних технологій ХНТУ.
Наукові інтереси: людино-машинна взаємодія, інформаційна безпека.
e-mail: bbbosss@i.ua

МАЗМАНЯН Сергій Русланович
Студент кафедри інформаційних технологій ХНТУ.
Наукові інтереси: людино-машинна взаємодія, тривимірна графіка, інформаційна безпека.
e-mail: sergey.mazmanian@gmail.com

ЛЕВИЦЬКА Анна Михайлівна
Студентка кафедри інформаційних технологій ХНТУ.
Наукові інтереси: людино-машинна взаємодія, інформаційна безпека, тривимірна графіка.
e-mail: good.anna.marya@gmail.com

В сучасному світі з великою інформаційною завантаженістю, коли кожен день ЗМІ повідомляють про хакерські атаки на інформаційні ресурси державних установ та викрадення персональних даних різних організацій та приватних осіб, безпекою не опікуються лише вкрай недалекоглядні користувачі.

У жовтні 2016 року кількість підключень до сайтів з мобільних пристроїв у всьому світі вперше перевищила використання Інтернету зі стаціонарних комп'ютерів і ноутбуків, свідчать дані аналітичної компанії StatCounter. Частка мобільних пристроїв в жовтні 2016 року склала 51,3% від загальної кількості пристроїв, яка використовують Інтернет.

Серед персональних комп'ютерів/ноутбуків та мобільних пристроїв найбільш розповсюдженим типом інтернет з'єднання є стандарт 802.11(Wi-Fi).

Більшість користувачів не здогадується, що кваліфікований зловмисник може заволодіти персональними даними користувача ноутбука або смартфону на базі Андроїд або IOS, використовуючи стандартні пакети спеціалізованих програм, що знаходяться у вільному доступі.

ПОСТАНОВКА ЗАДАЧІ

Задачами розглянутого у статті дослідження є:

- аналіз безпеки інтерфейсу бездротових мереж зі стандартом шифрування WPA / WPA2,

- класифікація та кластеризація паролів, які були застосовані користувачами при аутентифікації.

Дані для дослідження були зібрані з відкритих джерел, зокрема [1], а також з анонімного опитування студентів ХНТУ спеціальності 121 «Інженерія програмного забезпечення» (понад 40000 паролів).

Класифікація та кластеризація проведена на основі запропонованих авторами стереотипів паролів.

ОСНОВНА ЧАСТИНА

До WPA, що був визначений в специфікації 802.11i, для забезпечення безпеки бездротових з'єднань використовувався WEP. Пізніше, після масових розкрадань персональних даних користувачів (зокрема номера кредитних карт), з'ясувалося що алгоритм шифрування WEP досить вразливий і було розроблено алгоритм WPA. Незабаром, після повсюдного впровадження WPA

шифрування, WEP було визнано застарілим, та не рекомендовано до використання[2].

Специфікація 802.11i складається з трьох основних частин, організованих у 2 рівні. Це зображено у таб.1

Таб. 1

Структура специфікації 802.11i

802.1x	
RC4-based TKIP	AES-based CCMP

Нижній рівень представлений алгоритмами шифрування, такими як Temporal Key Integrity Protocol (TKIP) та CBC-MAC protocol (CCMP). Задля зворотної сумісності з WEP, TKIP використовує швидкий потоковий алгоритм шифрування RC4. CCMP базується на Advanced Encryption Standart (AES) – одному з найпопулярніших алгоритмів шифрування із симетричним ключем.

На верхньому рівні лежить 802.1x, що є стандартом портового контролю доступу. 802.1x забезпечує надійну аутентифікацію та поширення ключа шифрування. Обидва компоненти були відсутні у початковому стандарті 802.11[3].

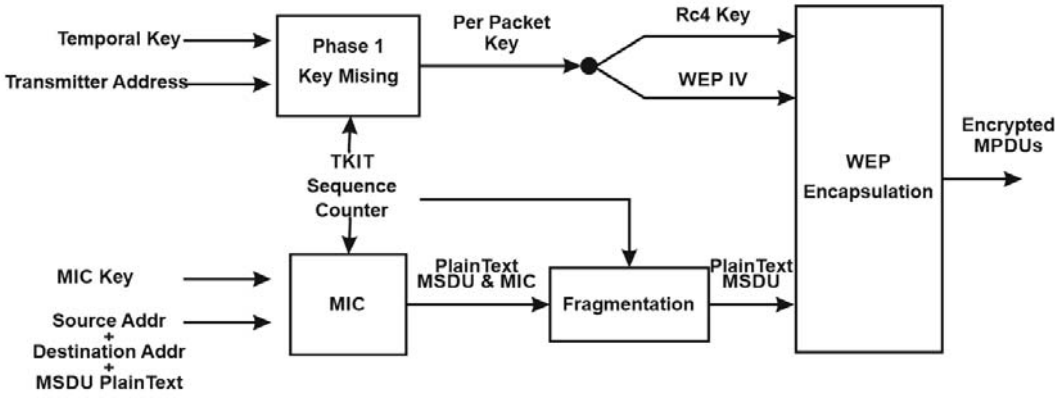

Рис. 1 Алгоритм шифрування за протоколом TKIP

Протокол TKIP (Temporal Key Integrity Protocol - протокол тимчасової цілісності ключа) виконує функції забезпечення конфіденційності і цілісності даних. Функціонально TKIP є розширенням WEP. Аналогічно з WEP, у ньому використовується алгоритм шифрування RC-4, але більш ефективний механізм управління ключами. Протокол TKIP генерує новий секретний ключ для кожного переданого пакета даних. Відрізняється також і механізм генерації ключа – його отримують із трьох компонентів: базового ключа довжиною в 128 біт (TK), номеру переданого пакета (TSC) та MAC-адреси пристрою-передавача (TA). Також в TKIP використовується 48-розрядний вектор ініціалізації (IV - initialization vector). Для уникнення повторного використання IV використовується наскрізний лічильник пакетів (TSC) довжиною 48 біт. Він постійно збільшується, скидаючись в 1 тільки при генерації нового ключа. Молодші 16 біт TSC включаються в новий IV (рис. 2)[4].

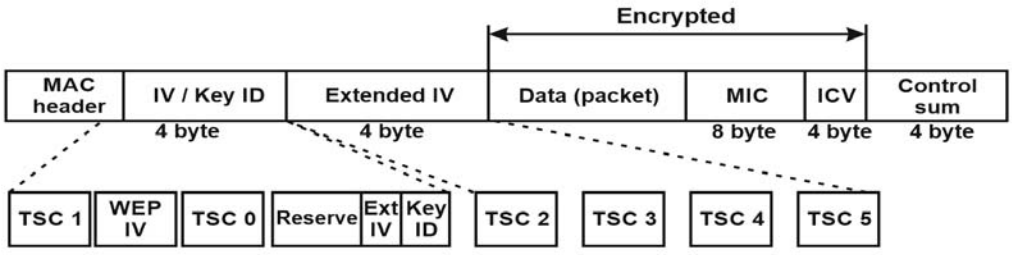

Рис. 2 Пакет після шифрування TKIP

Основна відмінність CCMP від TKIP і WEP – централізоване управління цілісністю пакетів, яке виконується на рівні AES. Пакет CCMP збільшений на 16 октетів, заголовок складається з трьох частин: PN (номер пакета, 48-розрядний), ExtIV (вектор ініціалізації), та ідентифікатора ключа (рис. 3). Алгоритм інкапсуляції даних з використанням CCMP:

1. Номер пакета збільшується на якесь число, щоб уникнути повторення пакетів;

2. Створюйте нові аутентифікаційні дані;

3. Створити службове поле nonce;

4. Номер пакета і ідентифікатор ключа поміщаються в заголовок пакета;

5. Поле nonce і додаткові аутентифікаційні дані шифруються з використанням тимчасового ключа.

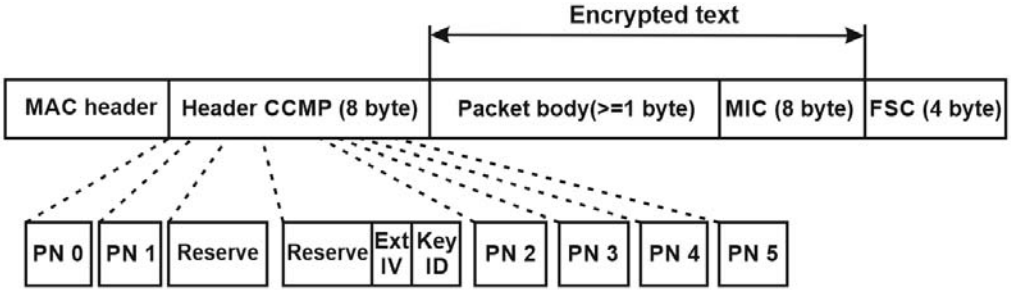

Рис. 3 Структура зашифрованого пакету WPA2

Алгоритм декапсуляції даних з використанням CCMP:

1. Створюються поля додаткових ідентифікаційних даних та поле nonce з використанням даних пакета;

2. Поле додаткових ідентифікаційних даних витягується з заголовка зашифрованого пакета;

3. Витягується поле A2, номер пакета та поле пріоритету;

4. Витягується поле MIC;

5. Виконується розшифровка пакета та перевірка його цілісності, з використанням шифротексту пакета, додаткових ідентифікаційних даних, тимчасового ключа та власне MIC;

6. Виконується збірка пакета в розшифрованому вигляді;

7. Пакети з повторюваним номером відкидаються.

Даний метод шифрування в бездротової мережі на даний момент є найбільш надійним.

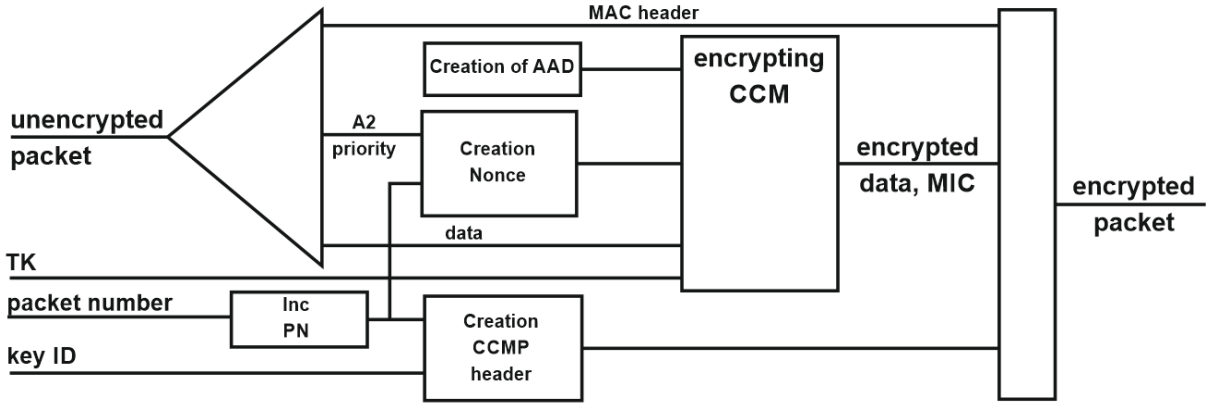

Рис. 4 Структурна схема протоколу шифрування CCMP

Корпоративна бездротова локальна мережа (WLAN) складається з трьох основних об'єктів – автентифікатор або точка доступу (AP) у 802.11, клієнтський пристрій у 802.11 та сервер автентифікації (AS). Автентифікатор – це порт, який забезпечує автентифікацію та спрямовує трафік відповідним об'єктам в

мережі. Клієнтський пристрій – порт, що має доступ до мережі. Сервер автентифікації виконує фактичну автентифікацію. AS може бути в AP або бути підключеним до дротової мережі. Сервер RADIUS – це типовий AS, який використовується сьогодні.

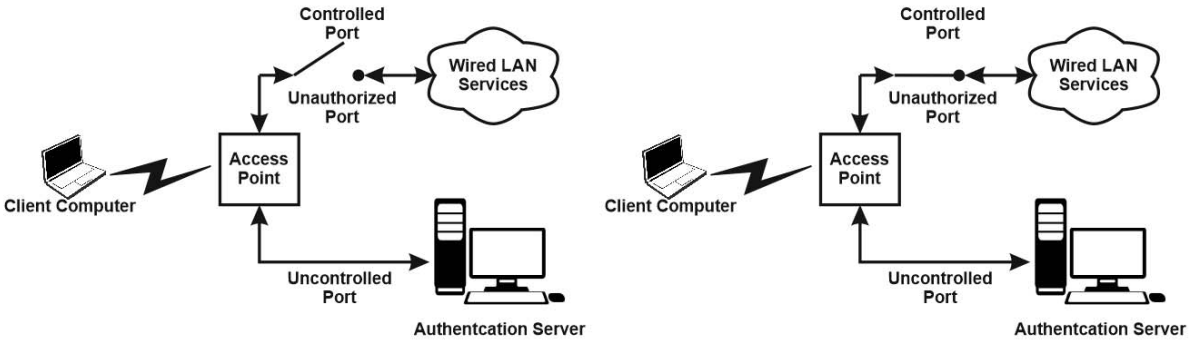

Рис. 5 Спрощена схема устрою мережі WLAN

Перш ніж авторизований заявник може дозволити спілкуватися з АС після його санкціонування, заявник може отримати доступ до інших ресурсів у мережі. Процес аутентифікації є взаємним. І клієнт, і мережа повинні довести свою ідентичність[3,4].

Є два види ключів в мережі з підтримкою 802.1x:

1. Сеансовий ключ або парний ключ. Сеансовий ключ використовується лише між клієнтом та його AP.

2. Груповий ключ. Груповий ключ генерується один на всіх клієнтів, підключеними одного AP. Він використовується для багатоадресного трафіку.

Якщо у корпоративних мережах стандарту 802.11 способи авторизації можуть бути різними, то в повсякденному житті надання користувачу доступу до мережі відбувається після введення кодової фрази (пароля), довжиною від 8 до 63 символів[1,5,6].

За визначенням стандарту WPA і умови дотримання винятків прошивки деяких роутерів досліджені паролі в загальному випадку можна розділити на сім великих груп:

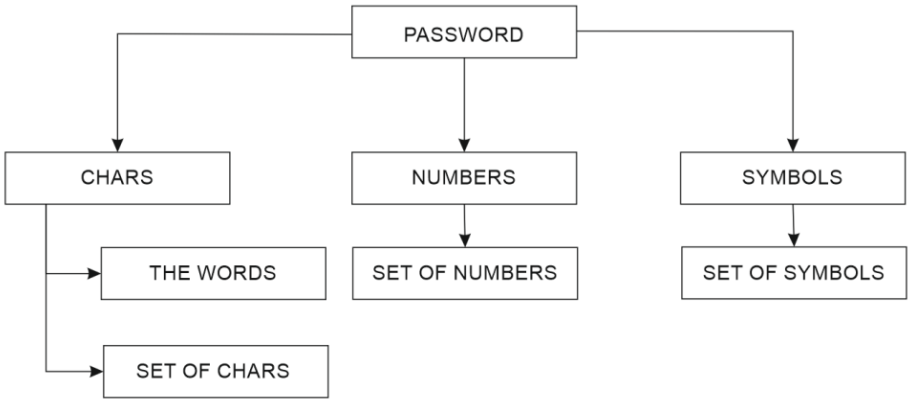

Рис. 6 Основні стереотипи паролів

Як видно на рисунку 6, основу класифікації паролів складають три великі групи: «букви», «цифри» і «спеціальні символи», які в свою чергу діляться на: «слова», «набір букв», «набір цифр» і «набір символів », з яких складаються різні комбінації, такі як «множина символи + цифри», «множина символи + літери» тощо.

У числовому співвідношенні дані наведені на рис.7:

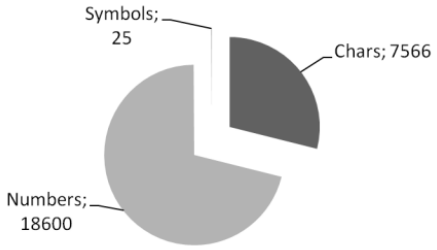

Рис. 7 Діаграма 1

З наведеної діаграми можна зробити висновок про те, що серед паролів, які складаються з однотипного набору (цифри, букви або спеціальні символи (далі просто символи) переважають числові. Тобто при виборі пароля (секретного слова) користувачі віддають перевагу набору з цифр . Які це набори буде розглянуто пізніше.

Значну частину (близько 1/3) всіх проаналізованих стереотипів паролів складають комбіновані стереотипи (рис.8).

Рис. 8 Діаграма 2

Співвідношення між цифровими і комбінованими стереотипами приблизно однаково (рис.9):

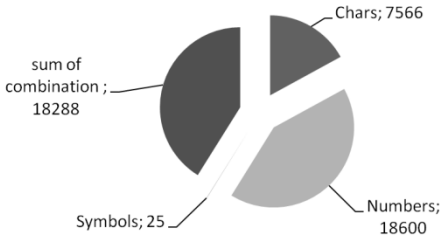

Рис. 9 Діаграма 3

Авторами статті були виділені (і в подальшому підтверджені експертами) такі стереотипи паролів:

- 8 цифр (в тому числі дати / дати народження),
- набір букви + цифри,
- слово + набір цифр,
- 10 цифр або більше, в тому числі номери телефонів,
- 1 слово,
- 2 слова,
- набір букв,
- ім'я + набір цифр,
- ім'я + дата / дата народження,
- 9 цифр,
- 3 слова або більш,
- набір букви + цифри + символи,
- слово + символи,
- слово + цифри + символи,
- набір цифр + символи,
- набір букви + символи,
- дата / дата народження + набір символів,
- набір символів.

Зв'язки між простими і складними стереотипами паролів представлені на рис. 10.

В таб. 2 наведені кількісні значення кожного з стереотипів.

Таб. 2

Кількісні значення стереотипів паролів

Кількість	Стереотип
14136	8 numbers
7882	Set of chars + Set of numbers
7284	The words +Set of numbers
3710	10 numbers or more
3121	1 word
2533	2 words
1241	Set of chars
1109	Name+Set of numbers
932	Name +Date/Birthday
754	9 numbers
671	3 words or more
517	Set of chars +Set of numbers +Set of symbols
190	The words + Set of symbols
160	The words + Set of numbers + Set of symbols
122	Set of Numbers+Set of symbols
53	Set of chars + Set of symbols
39	Date/Birthday +Set of symbols
25	Set of symbols
44479	Total

Вочевидь, найбільш популярними у використанні є паролі з 8-ми цифр. До цього числа входять дати, дні народження (наприклад, 14121997), як найпопулярніший стереотип, пін-код від WPS роутера, який встановлений паролем за замовчуванням. Частота використання 8-ми цифр пов'язана ще з стереотипністю мислення самого користувача і особливостями пам'яті

людини. Набагато простіше запам'ятати «що є паролем», ніж посимвольного значення. При налаштуванні роутера BIOS запитує користувача ввести пароль з мінімум (!) 8-ми символів і максимум 63-х. Цей факт є причиною великої частоти використання не тільки стереотипу пароля «8 цифр», а також і стереотипу «набір символів + набір цифр». Тут одним з лідерів за частотою використання є «4 букви + 4 цифри». У цьому стереотипі очікувано повторюється стереотипність мислення користувача, так як був запит на введення мінімум 8-ми символів.

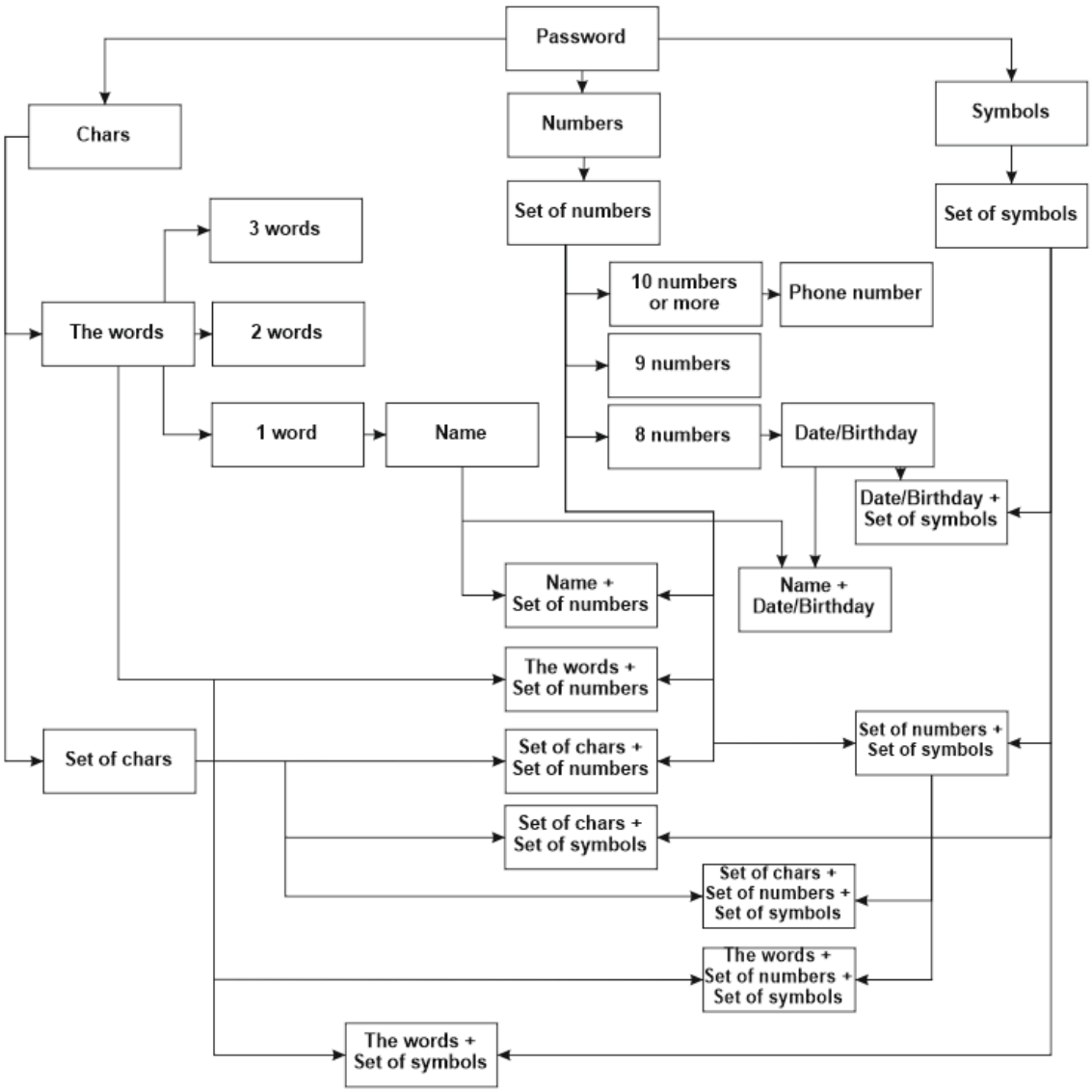

Рис. 10 Класифікація стереотипів паролів

Як приклад стереотипу «4 букви + 4 цифри» розглянемо набір «abcd1234». Набором символів найчастіше є якась абревіатура, що легка для запам'ятовування користувачем, така як «sssr» або «ODMA», а в якості цифр, як правило, виступає рік - «1998», але іноді зустрічаються «lena1234».

На третьому місці за популярністю знаходиться стереотип «слово + набір цифр». В якості слова може виступати як власна назва, так і слово з загальновживаної мови, з повсякденного спілкування. Наприклад: «password123456» або «partkom1». Складність розшиф-

ровки подібних стереотипів невелика і буде розглянута нижче.

Стереотип «10 цифр і більш» являє собою, найчастіше, номер мобільного телефону, що складається з коду оператора (3 цифри) і самого номера (7 цифр). У цей набір може входити також код країни. При уявній складності розшифровки через довжину, насправді даний стереотип обчислюється за пару годин, в залежності від потужності відеокарти.

Для наочності наведемо таблицю частоти використання всіх наведених стереотипів паролів у вигляді діаграми (рис.11):

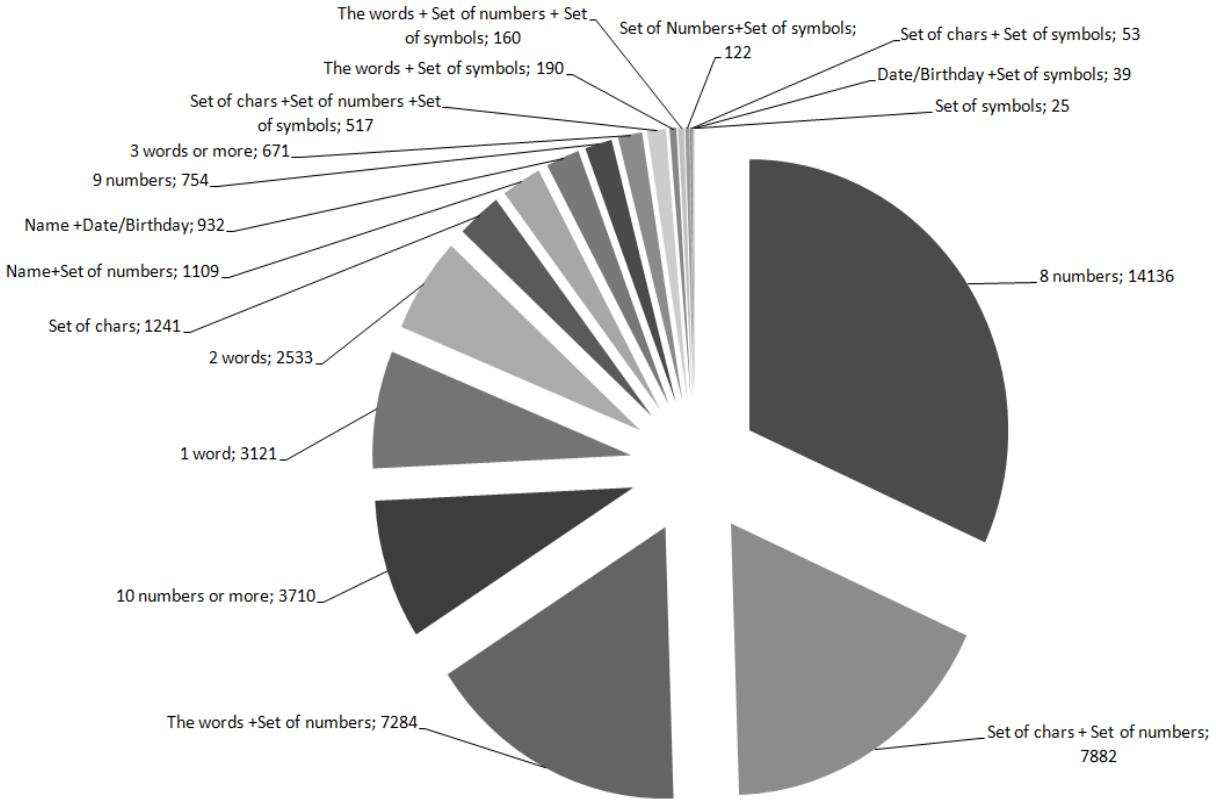

Рис. 11 Діаграма 4

З рис.11 і з даних відсортованої таб.2 нескладно помітити, що частота використання простих стереотипів набагато вище, ніж складних. Що зайвий раз свідчить про занижений рівень інформаційної культури більшості користувачів і необізнаності про можливі види атак на їхні персональні дані через уразливість використовуваного пароля. Характерними представниками складних стереотипів можна назвати «два слова», «три слова», «слово + набір символів», «слово + набір символів + набір символів» (рис.12).

Як видно з діаграми частоти використання складних стереотипів беззаперечну перевагу користувачами віддається «набору букв + набір цифр» і «слову + набір цифр». Це цілком природно пояснюється тим, що користувачеві простіше запам'ятати такий пароль. Як характерні приклади таких стереотипів можна розглядати «abrakadabra123456789».

Одним з найшвидших інструментів по відновленню паролів визнаний Hashcat [7,8]. Одна з різновидів мультиплатформенна oclHashcat використовує CUDA технології. CUDA - це архітектура паралельних обчислень від NVIDIA, що дозволяє істотно збільшити обчислювальну продуктивність завдяки використанню GPU (графічних процесорів).

OclHashcat відновлює безліч хеш-функцій (MD4, MD5, Half MD5, SHA1 і т.д., повний список на офіційному сайті Hashcat [8]), включаючи WPA / WPA2, з використанням Multi-GPU (до 128 GPU!).

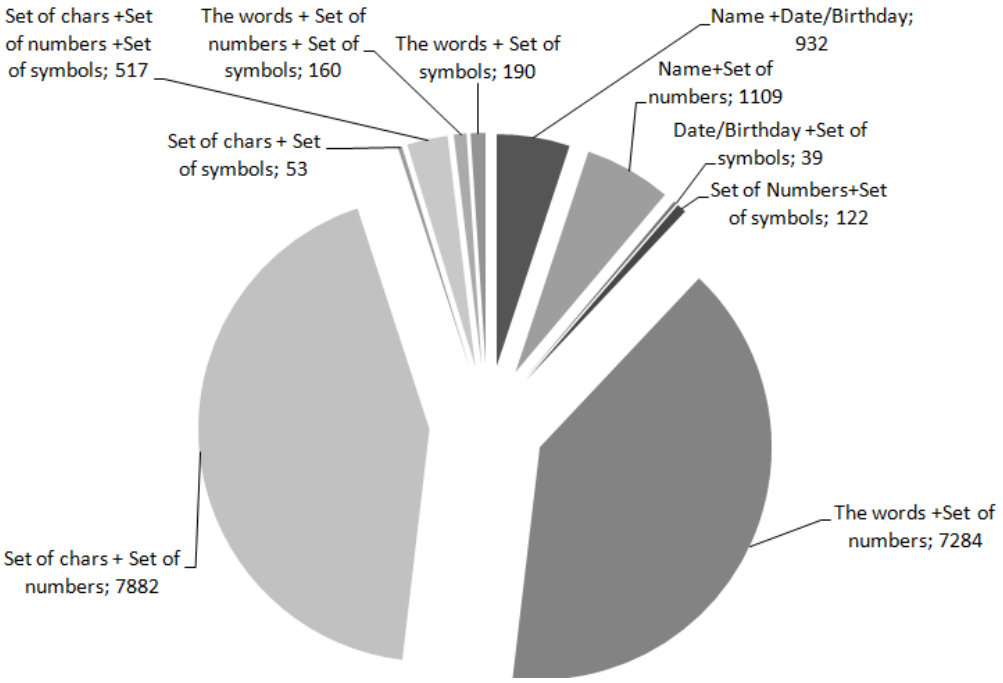

Рис. 12 Діаграма 5

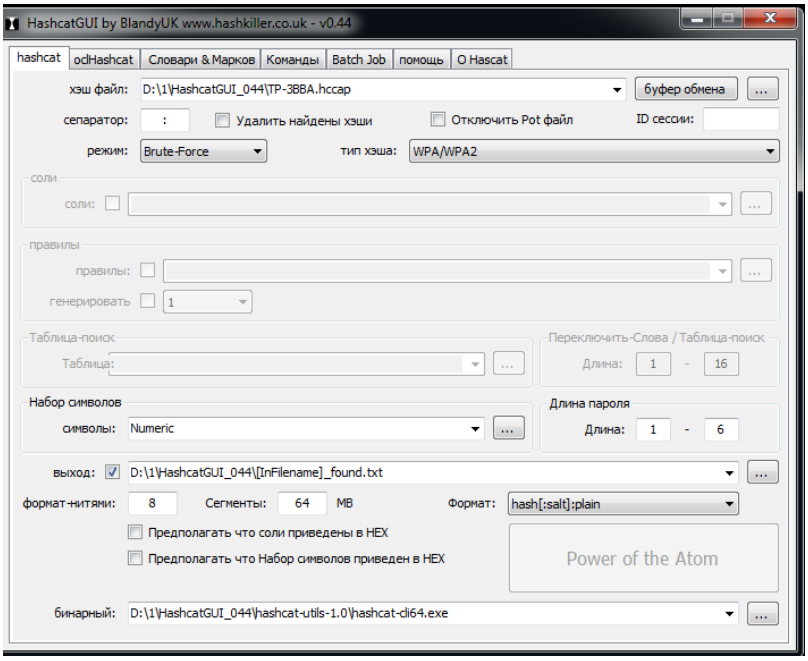

Рис. 13 Загальний вигляд GUI oclHashcat

Атаки проводяться за такими модами (рис.14):
- Straight (прямий перебір по словнику / списку словників), рис.15;
- Combination (комбінація двох словників);
- Brute-force (перебір по масці);
- Hybrid dict + mask (перебір по масці + словник), рис.16;
- Hybrid mask + dict (перебір по словнику + маска).

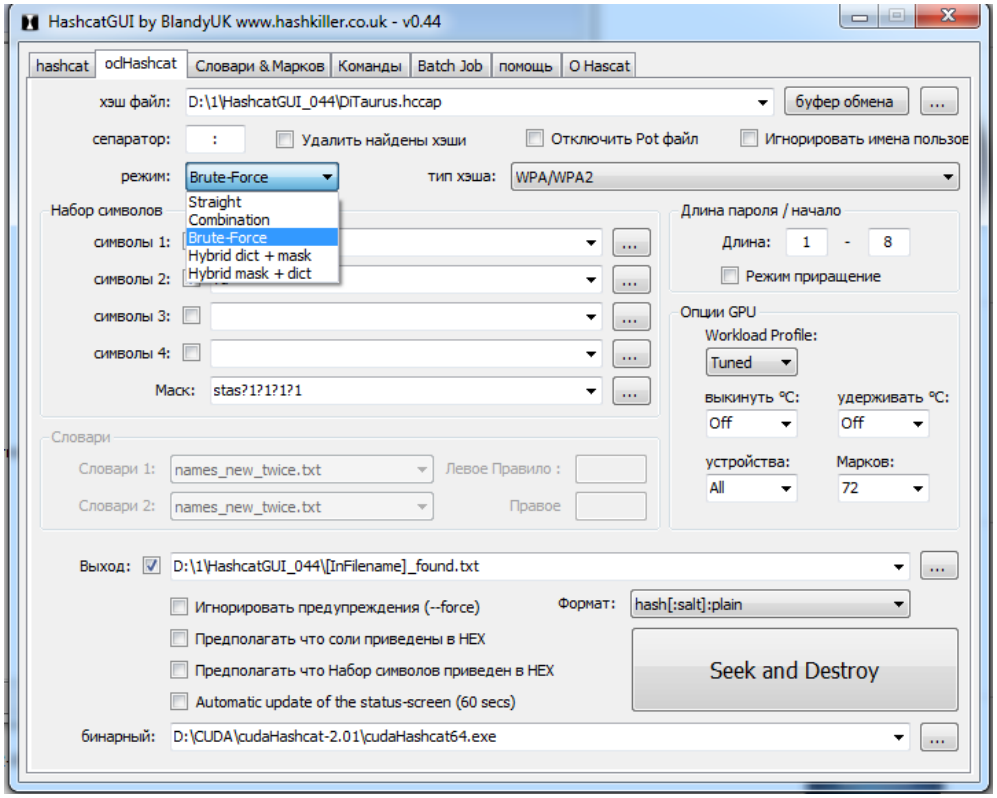

Рис. 14 Вибір типу атаки

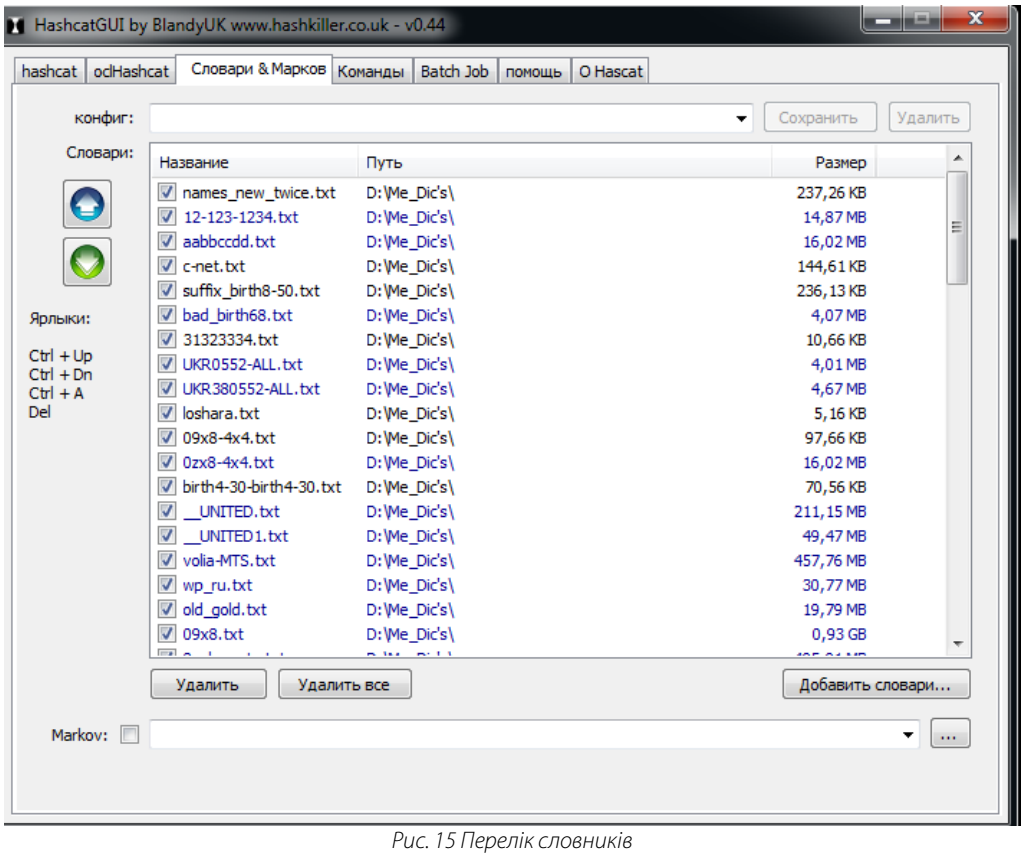

Рис. 15 Перелік словників

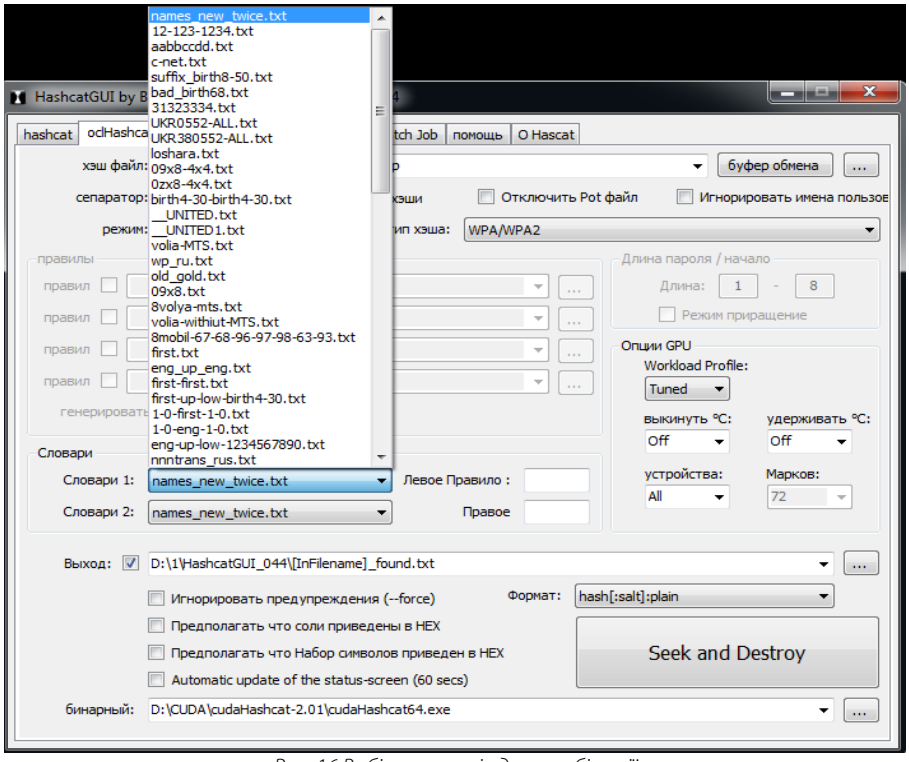

Рис. 16 Вибір словників для комбінації

На сьогоднішній день це найбільш потужний інструмент для відновлення / проведення атак на паролі. Остання версія v4.1.0 / 2018.02.21 знаходиться у вільному доступі на ресурсі [8].

В рамках даного дослідження використовувалася відеокарта GeForce GT 750M, яка при переборі за словником показує швидкість близько 18000 хешів за секунду (рис.17).

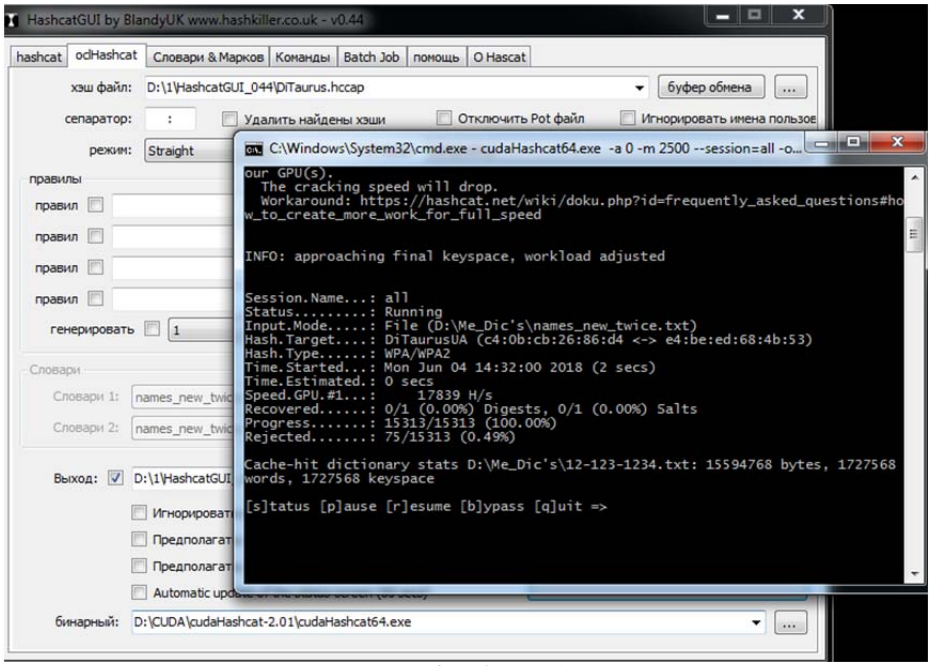

Рис. 17 Приклад роботи oclHashcat

При даній швидкості перебору паролів список дат від 01.01.1950 в форматі дд / мм / рр (наприклад «13031997») буде перерахований за 1 секунду. Що свідчить про те, що використання дат в форматі дд / мм / рр, або навіть з роздільниками, неприйнятно в рамках дотримання елементарних правил безпеки.

Використання в якості пароля номера мобільного або стаціонарного телефону також небезпечно, так як зловмисникові потрібно всього лише пара годин для перебору всіх мобільних операторів і комбінацій номерів. При цьому довжина пароля буде вагомою, 10 або 12 цифр і недосвідчений користувач вважатиме його досить надійним, але з використанням «стереотипного» (запропонованого авторами дослідження) підходу для підбору пароля зловмисник вирахує його досить швидко.

Розглянемо ще один приклад складного пароля «Volodymyr12091964». При уявній надійності стереотипу в 17 символів, посимвольний підбір якого займе не одну тисячу років, він досить простий з точки зору стереотипного підходу задля розшифровки WPA паролів, так як перебір згенерованого словника «ім'я + дата» займе менше години.

ВИСНОВКИ

Алгоритм шифрування WPA/WPA2 можна вважати достатньо надійним, але частина безпеки в бездротових з'єднаннях покладається на користувача. Тому безпека в бездротових з'єднаннях в більшій мірі залежить від надійності пароля. Нажаль, аналіз класифікації вживаних паролів свідчить про те, що більшість користувачів використовує ненадійні паролі, нехтуючи безпекою своїх персональних даних, та даних компаній та організацій.

Вибірку паролів можна вважати легітимною, збір даних проводився впродовж декількох років, в різних країнах і серед користувачів різних вікових категорій. Кількість зібраних даних можна вважати достатньою.

Деякі користувачі помилково вважають, що надійність залежить виключно від довжини паролю, але не усвідомлює, що зловмисник може використовувати стереотипний підхід.

Запропонований в статті метод класифікації та кластеризації паролів, які були застосовані користувачами при аутентифікації в бездротових мережах зі стандартом шифрування WPA / WPA2, значно скорочує час на підбор паролю.

В якості способу відновлення хешу паролю безальтернативно запропоновано використовувати oclHashcat, обчислювальні здатності якого значно перевищують навіть останні найпотужніші процесори в десятки разів, за рахунок використання CUDA технологій, в залежності від класу відео карти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Distributed WPA PSK auditor [Yelektronniy resurs] // Distributed WPA PSK auditor URL: https://wpa-sec.stanev.org/?dicts (data zvernennya 10.02.18).
2. Zegzhda D., Ivashko A.M. Osnovy bezopasnosti informatsionnykh sistem. – M.: Goryachaya liniya – Telekomyu 2008. – 452 s.
3. P. Roshan, Dzh. Lieri. Osnovy postroyeniya lokal'nykh setey standarta 802.11. – Per. s angl. – M.: Izdatel'skiy dom «Vil'yams», 2004. – 296 s.
4. Tomas Maufer. WLAN: prakticheskoye rukovodstvo dlya administratorov i professional'nykh pol'zovateley. – M.: KUDITS-Obraz, 2005. – 368 s.
5. Penetration Testing Services [Yelektronniy resurs] // Offensive Security. 2018. URL: https: https://www.offensive-security.com/offensive-security-solutions/penetration-testing-services/ (data zvernennya 11.03.18).
6. Official site of Wi-Fi Alliance [Yelektronniy resurs] // Wi-Fi Test Suite 2018. URL: https://www.wi-fi.org/certification/wi-fi-test-suite (data zvernennya 11.03.18).
7. Instrumenty Kali Linux [Yelektronniy resurs] // © 2018 Instrumenty Kali Linux. All Rights Reserved. URL: https://kali.tools/?p=538 (data zvernennya 11.05.18).
8. Hashcat advanced password recovery [Yelektronniy resurs] URL: https://hashcat.net/hashcat/ (data zvernennya 11.05.18).
9. Malyuk, A.A. Informatsionnaya bezopasnost': kontseptual'nyye i metodologicheskiye osnovy zashchity informatsii: Uchebnoye posobiye dlya vuzov. / A.A. Malyuk. - M.: Goryachaya liniya -Telekom , 2004. – 280 c.
10. Shan'gin, V.F. Informatsionnaya bezopasnost' i zashchita informatsii / V.F. Shan'gin. - M.: DMK, 2014. - 702 c.
11. Chipiga, A.F. Informatsionnaya bezopasnost' avtomatizirovannykh sistem / A.F. Chipiga. - M.: Gelios ARV, 2010. - 336 c.

Рецензент: д.т.н., проф. Ходаков В.Е.

Херсонский национальный технический университет