БЕЗПЕЧНА КОММУНІКАЦІЯ В БЕЗДРОТОВИХ МЕРЕЖАХ WI-FI

Геращенко В.Д.

студент 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Wi-Fi (Wireless Fidelity) – технологія бездротової локальної мережі з основними діапазонами 2.4 ГГц (2412 МГц – 2472 МГц) та 5 ГГц (5160 – 5825 МГц) для взаємодії з мобільними пристроями [1].

Бездротові мережі мають достатньо велике поширення. У зв'язку з цим, кожен користувач має вміти організовувати безпечну комунікацію своєї мережі. Для забезпечення безпечного обміну даними у бездротових мережах було розроблено декілька основних технологій шифрування:

1. WEP – технологія шифрування, яка була розроблена у 1997 році Інститутом інженерів електротехніки та електроніки. Алгоритм забезпечував конфіденційність та захист персональних даних від неавторизованих користувачів із допомогою поточного шифру RC4, що мав високу швидкість шифрування [2].

2. WPA – технологія першого покоління, розроблена у 2003 році та була використана для заміни технології WEP, бо мала посилену безпеку даних та більш строгий контроль над користувачами. Технологія мала гарну сумісність з великою кількістю пристроїв на програмному та апаратному рівні. Для шифрування WPA використовує протокол EAP [2].

3. WPA2 – технологія розроблена у 2004 та є другим поколінням WPA. У цьому поколінні покращили шифрування за допомогою протоколів CCMP та AES. За лік чого була багаторазово підвищена безпека комунікації у бездротовій мережі. У наш час технологія є найбільш популярною та з 2006 року є обов'язковою для сертифікованих приладів Wi-Fi [2].

Покращення безпечної комунікації у бездротових мережах

Здебільшого, організація безпеки бездротової мережі залежить від навичок її власника (адміністратора).

По-перше, варто встановлювати багатосимвольні паролі з використанням малого і великого регістру з додаванням спеціальних символів юнікоду. Це допоможе багаторазово збільшити час брутфорсу (методу грубого перебору паролів).

По-друге, необхідно бути обережним із фішингом. Сучасні набори інструментів, дозволяють блокувати будь-яку точку доступу Wi-Fi та робити її копії, які можуть маскуватися під назвою власника точки доступу але не мають паролю для підключення. В жодному разі не можна вводити свої паролі при підключені та у вебінтерфейсу фейкової точки доступу [3].

Основні види атак на точку доступу

Сучасні зловмисники переважно використовують метод деаутентифікації у комбінації з фішингом чи підбором хеш-суми. Атака методом деаутентифікації відправляє пакети для роз`єднання із точкою доступу одному чи групі її

користувачів. Ця атака може використовуватися для:

- встановлення назви схованої точки доступу;
- нескінченної відправки пакетів деаунтифікації, що приводить до неможливості користування точкою доступу;
- перехвату рукостискань WPA/WPA2;
- генерації ARP запитів [4].

Протокол ARP призначений для ідентифікації MAC-адреси за допомогою IP-адреси іншого комп'ютеру. Він дозволяє пристроям комунікації у локальній мережі робити запит на визначення якому приладу назначена конкретна IP-адреса.

Генерація ARP запитів дозволяє перехоплювати увесь трафік та *cookie*-файли потенціальної жертви за допомогою яких, наприклад, можливо увійти у недавно відвідані соціальні мережі і т.д. Для ефективного захисту від ARP атаки можна зарезервувати IP-адресу за MAC-адресою у відповідному інтерфейсі маршрутизатора. Також, існує програмний захист Ethernet-портів за допомогою функції DAI (функція перевірки підміни пакетів). Вона дозволяє оцінити достовірність кожного ARP-запиту та відкинути зловмисні пакети [4].

Розрахунок часу взлому паролів

Після перехвату рукостискань, зловмисник має підібрати пароль точки доступу за допомогою готових чи згенерованих словників [5].

Для перебору восьми символьного паролю, який складається тільки з цифр необхідно перебрати 10^8 = 100000000 паролів. Якщо використовувати середньостатистичний комп'ютер із дискретною відеокартою, то можливо досягти швидкості перебору понад 400 тис. паролів у секунду. Це означає, що усі восьмисимвольні чисельні паролі можливо зламати лише за 250 секунд. Тому, задля покращення надійності необхідно використовувати багатосимвольні паролі з комбінації чисел, латинських букв малого та великого регістру. Наприклад, для підбору паролю, який складається з двадцяти різних символів зі швидкістю 10 мільйонів паролів у секунду, зловмиснику може знадобиться понад 31 мільйонів років [6].

Список використаних джерел:

1. Що таке Wi-Fi? URL: https://www.newscientist.com/question/what-does-wi-fi-stand-for/
2. Різниця між WEP, WPA, WPA2 алгоритмів безпеки. URL: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
3. Фішинг та безпека у мережі Wi-Fi. URL: https://aircrack-ng.blogspot.com/2020/01/aircrack-ng-16.html
4. ARP запити, використання та захист. Отруєння ARP. URL: https://datatracker.ietf.org/doc/html/rfc2002
5. Метод грубого перебору паролів. URL: https://ieeexplore.ieee.org/abstract/document/8400211
6. Розрахунок надійності паролів. URL: https://www.mecs-press.org/ijcnis/ijcnis-v8-n7/IJCNIS-V8-N7-4.pdf

Науковий керівник: доцент Задерейко О.В.