МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

УДК 004.056.53

АНАЛІЗ ШИФРІВ У БЕЗДРОТОВИХ МЕРЕЖАХ

КУЛЯ Ю. Е. (*yuliia.kulia@nure.ua*)
Харківський національний університет радіоелектроніки
ГАВРИЛОВА А. А. (*alla.gavrylova@hneu.net*)
Харківський національний економічний університет імені Семена Кузнеця

Розглянуто особливості відомих методів шифрування в бездротовій мережі Wi-Fi. Проаналізовано їх відмінності з точки зору криптостійкості, вразливостей і наслідків проведених атак. Зроблено висновок про можливість використання алгоритму шифрування WPA3 різними групами користувачів безпроводових мереж.

Бездротові мережі є невід'ємною частиною корпоративної інфраструктури більшості сучасних компаній. Це пояснюється тим, що використання Wi-Fi дозволяє розгортати мережі без прокладки кабелю. Розгорнута бездротова мережа дозволяє організувати високошвидкісний доступ в Інтернет швидко і комфортно. Однак небезпечне використання або адміністрування бездротових мереж всередині організації тягне за собою серйозні загрози. Успішний злом Wi-Fi дозволяє не тільки перехоплювати чутливу інформацію, атакувати користувачів бездротової мережі, але і розвивати атаку для отримання доступу до внутрішніх ресурсів. Дані небезпеки в корпоративному сегменті тягнуть за собою збитки для бізнесу та окремих користувачів, розмір який може бути величезним.

У зв'язку з цим актуальним є пошук шляхів захисту проводових мереж через механізми аутентифікації і шифрування, які зазнають різні зміни у зв'язку з появою нових стандартів, що відповідають за безпеку інформації в сучасному кіберпросторі.

Для представлення один одному і підтвердження прав на обмін даними між клієнтами і точками доступу, використовуються такі механізми аутентифікації, як відкрита аутентифікація, аутентифікація із загальним ключем, WPA (Wi-Fi Protected Access) і WPA2 [1]. Суть першого механізму полягає в тому, що передбачається захист бездротової мережі на основі MAC-фільтрації. Суть другого механізму полягає в підтвердженні на авторизацію від точки доступу асоціації зашифрованої послідовності із запитом клієнта. Третій і четвертий механізми аутентифікації здійснюються за допомогою зовнішнього сервера з даними клієнтів і завчасно наданого ключа, встановленого на точку доступу.

Серед механізмів шифрування крім вже відомих WPA і WPA2, набирає популярність WPA3 [2] (табл. 1). WPA був надбудовою над WEP (Wired Equivalent Privacy), який дозволяв усунути вразливість у WEP, пов'язану з недостатнім розміром вектора ініціалізації без заміни обладнання. Першою ідеєю була зміна ключів [2]. Основою для цього став протокол TKIP (протокол цілісності тимчасового ключа). Він значно посилював WEP за допомогою дворівневої системи векторів ініціалізації. Іншим нововведенням у WPA стала технологія WPS (Wi-Fi Protected Setup), яка дозволяє бездротовим пристроям спрощено отримати доступ до Wi-Fi за умови фізичного доступу до маршрутизатора. Вона ж і стала першою експлуатованою вразливістю WPA. Ще одна уразливість ховалася в особливості ключів TKIP, яка дозволяє їх зламати за 12 – 15 хвилин з використанням утиліти Aircrack-ng, а також деяких математичних напрацювань. У 2006 році в результаті успішних атак, заснованих на знанні деяких даних в зашифрованих фреймах, надійність WPA була повністю скомпрометована. WPA2 до моменту повної компрометації WPA був уже реалізований у багатьох бездротових пристроях. Для даного алгоритму було характерно індивідуальне шифрування даних кожного користувача і надійний алгоритм шифрування AES (Advanced Encryption Standard).

Таблиця 1

Порівняння алгоритмів шифрування для бездротових мереж

Характеристики	WPA	WPA2	WPA3
Рік випуску	2003	2004	2018
Метод шифрування	Temporal Key Integrity Protocol (TKIP)	Advanced Encryption Standard (AES)	Advanced Encryption Standard (AES)
Рівень безпеки	більший, ніж у WEP, пропонує базовий рівень безпеки	більший, ніж у WPA, пропонує підвищений рівень безпеки	більш надійна автентифікація та високий рівень криптостійкості для високочутливих даних
Підтримка пристроїв	більш старіше програмне забезпечення	більш нове програмне забезпеченням	недоступно для деяких версій пристроїв
Довжина паролю	допускається коротший пароль	потрібно більш довгий пароль	потрібно більш довгий пароль
Користувачі	приватні користувачі	приватні користувачі та компанії	приватні користувачі та компанії
Вимоги для обчислювальних потужностей	мінімальні	більші потужності	великі потужності

Основними методами злому маршрутизаторів, які працювали по WPA2, був злом PIN-коду при підключенні через WPS або перехоплення рукостискання і підбір ключа методом підбору «грубою силою», нівелювати які вдалося відключивши WPS і встановивши досить сильний пароль. Уразливість hole196, яка призвела до реалізації атаки ARP/DHCP Spoofing, і розпочата в 2017 році атака KRACK, довели ненадійність протоколу WPA2. Новий протокол безпеки WPA3 був спробою усунути недоробки, що призвели до атак попередньої версії, за допомогою впровадження обов'язкової підтримки більш надійного методу з'єднання SEA (Simultaneous Authentication of Equals) (Dragonfly) [3], заснованому на протоколі обміну ключами Діффі-Хелмана з використанням кінцевих циклічних груп і використанні фреймів PMF, що забезпечили контроль цілісності трафіку.

Але, незважаючи на вжиті кроки щодо посилення захищеності бездротових мереж Wi-Fi, фахівці вважають, що пошук способу обходу PMF для примусового від'єднання клієнта від мережі не займе багато часу, а SEA тільки подовжить проведення словникових атак [4], і атакуючий зможе розгорнути свою точку доступу і перехоплювати трафік. Також впровадженню алгоритму WPA3 перешкоджають апаратні і потужністні обмеження. Оскільки є можливість використання даного алгоритму шифрування для різних груп користувачів, то інтерес до його застосування буде сприяти роботі надалі над ліквідацією існуючих недоліків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. П. Рошан, и Дж. Лиэри. *Основы построения беспроводных локальных сетей стандарта 802.11*. Москва, Россия: Вильямс, 2004.

2. В. Леонов, "Как ломаются беспроводные сети". [Электронный ресурс]. Доступно: http://citforum.ru/nets/wireless/crack. Дата обращения: Апр. 10, 2021.

3. О. И. Визавитин, Д. А. Логинова, и С. Д. Таякин, "Применение современных алгоритмов шифрования при обеспечении информационной безопасности беспроводных локальных сетей", *Молодой учёный* № 10(114)с. 138 – 141, 2016.

4. В. А. Шовкута, та С. В. Флоров, "Аналіз механізмів захисту та вразливостей бездротових WI-FI мереж" на Всеукр. наук.-практ. конф. Інформаційні технології. Безпека та зв’язок, Дніпро, 2016, с. 18 – 20.

УДК 004.056.5

ВИКОРИСТАННЯ СИСТЕМИ ДЛЯ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ В АНТИ-ФОРЕНЗИЦІ

МАКАРЕНКО А. О. (*makarenkoanton5@gmail.com*)
Харківський національний економічний університет імені Семена Кузнеця

Реферат. В умовах масової комп'ютеризації та зростання обсягу обороту даних, цифрова криміналістика привернула багато уваги останні десять років, незважаючи на те, що наукова галузь відносно зароджується. У всьому світі особливої актуальності набуває проблема злочинів в комп'ютерній сфері, за останні роки спостерігається істотне зростання числа зареєстрованих комп'ютерних злочинів і випадки комп'ютерного хуліганства із значним збитком.

Метою роботи є визначення методів антифорензіки, за допомогою генерування часткою секретних даних, представлених елементами секретних даних, на основі першого порогового значення кількості часткою, які дозволяють визначати секретні дані. Об’єкт дослідження – процес маскування інформації за допомогою криптографічних методів. Предмет дослідження – аналіз сучасного стану інформаційної безпеки на основі цифрової криміналістики і її підрозділу – антіфорензікі. Комп'ютерна криміналістика - це дисципліна, яка включає методи розслідування і аналізу для збору і збереження доказів з певного електронного або цифрового пристрою, який є підозрюваним у розслідуванні, таким чином, щоб докази підходили для подання в суді. Існують різні напрямки цифрової криміналістики, зображені на рис.1.

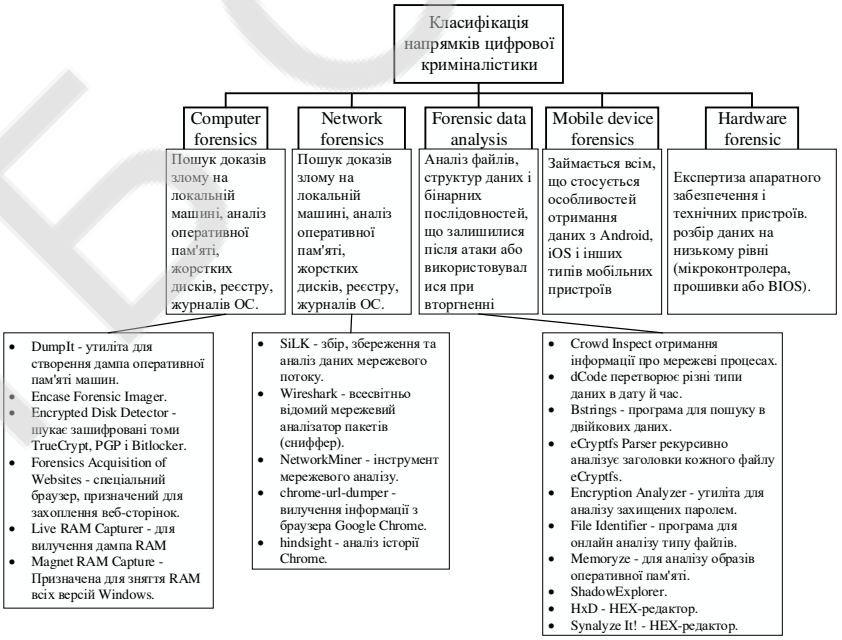

Рисунок 1 – Розділи форензіки

Пропонується спосіб генерації часток секретних даних, представлених елементами секретних даних, на основі першого порога кількості часткою, які дозволяють визначати секретні дані, спосіб включає: визначення часток секретних даних на основі секрету. елементи даних, один або кілька елементів випадкових даних, доданих до елементів секретних даних, і коефіцієнти систематичного коду з поділом на максимальну відстань

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.