Література

1. Бондаренко, Р.В. Технология NFC – связь на близком расстоянии / Р. В. Бондаренко // Электронные компоненты. – 2011. – №10. – С. 44–46.

2. Haselsteiner, E., Breitfuss, K.: Security in Near Field Communication (NFC) – strengths and weaknesses. In: Workshop on RFID Security 2006 (RFIDsec 06). Graz, Austria.

3. Фергюсон Н. Практическая криптография: [пер. с англ.] /Нильс Фергюсон, Брюс Шнайер. - М.: Диалектика; Вильямс, 2005.- 421 с.: а-ил.

Анотація

Представлені загрози безпеки технології NFC. Було показано, що захищеність від MITM-атак є серйозним фактором розвитку безпеки ближнього безконтактного зв'язку. На ньому заснований сучасний захист NFC за допомогою протокола Діффі-Гелмана. Створена модель специфічного узгодження ключів для NFC.

Ключові слова: NFC, MITM-атака, протокол Діффі-Гелмана, узгодження ключів.

Аннотация

Представлены угрозы безопасности технологии NFC. Было показано, что защищенность от MITM-атак является серьезным фактором развития безопасности ближней бесконтактной связи. На нем основана современная защита NFC с помощью протокола Диффи-Хеллмана. Создана модель специфического согласования ключей для NFC.

Ключевые слова: NFC, MITM-атака, протокол Диффи-Хеллмана, согласование ключей.

Abstract

The security threats of NFC-technology were presented in this article. It has been shown that protection from MITM-attacks is a major factor in the development of safety in near field communications. The modern protection of NFC is based on it through the Diffie-Hellman protocol. The model of specific key agreement for NFC was created.

Keywords: NFC, MITMA, Diffie-Hellman protocol, key-agreement.

БЕЗПЕКА WI-FI МЕРЕЖ

Лебединський М.О., студент, maksim.lebedinskiy@openmailbox.org;
Мащенко А.Г., студент, artemgennadievichmashenko@gmail.com;
Бойко В.В., старший викладач, glorytown@ukr.net
ДонНТУ, Красноармійськ, Україна

На сьогоднішній день проблема безпеки Wi-Fi мереж є найбільш актуальною. Безпеку треба розглядати з різних боків: екологічна та інформаційна безпека. Екологічна безпека – це вплив на середовище та вплив на інші мережі. Інформаційна безпека – це спосіб автентифікації та шифрування, який захищає мережу від проникнення зловмисників.

Деякі користувачі Wi-Fi пристроїв повідомляли, що мають проблеми зі здоров'ям при довгому використанні мережі Wi-Fi, але Всесвітня Організація Охорони Здоров'я інформує, що роковий сеанс впливу Wi-Fi ви-

промінювання, відповідає усього 20 хвилинам розмови по мобільному телефону [1]. Також було виявлено, що 3 місяця впливу випромінювання Wi-Fi точки доступу, приводять до серйозного погіршення здоров'я дерев. З міркувань екологічності є сенс обирати мінімальну потужність передавача, щоб забезпечувати мінімальний вплив на зовнішнє середовище. Також необхідно враховувати вплив інших мереж. Рекомендується зменшувати вплив передатчиків однієї мережі на іншу [2].

Послуги Wi-Fi потрібно надавати з необхідними показниками якості: це затримка, пропускна здатність, втрата пакетів та варіація затримки. На ці показники впливають такі параметри роботи Wi-Fi: Beacon Interval, DTIM interval, Ack Time Out, Power, Distance та автентифікація [3, 4, 5, 9].

Інформаційна безпека реалізується через автентифікацію (процедуру встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора) та шифрування (оборотне перетворення даних, з метою приховання інформації). Часто мережа Wi-Fi працює без автентифікації: у публічних місцях, таких як бібліотеки, аеропорти, вокзали, тощо [6]. Такі мережі необхідно захищати від розповсюдження вірусних програм, але у нашій роботі це не розглядається. В інших випадках рекомендується використовувати захищене з’єднання. Існує декілька найпоширеніших видів автентифікації. Це WPA PSK, WPA Enterprise, WPA2 PSK WPA2 Enterprise. Кожен з них має свої особливості та свої недоліки. В WPA та WPA2 використовують такі види шифрування, як AES та TKIP [7]. Якщо використовується автентифікація, то необхідно використовувати шифрування також, але шифрування знижує пропускну здатність, через збільшення робочої інформації пакета [2, 8, 11].

Причинами зниження швидкості можуть бути: Безліч різних Wi-Fi з’єднань, побутові прилади, налаштування безпеки, та застаріле ПЗ [2, 9, 10].

Для дослідження швидкості у мережі були проведені власні експерименти, результати яких відображені на рисунках.

Рисунок 1. Залежність від алгоритму автентифікації та типу шифрування при 100% потужності передачі

Згідно діаграми найкраще використовувати шифрування WPA2 AES, а найгіршу пропускну здатність має шифрування WPA TKIP. Пропускна здатність WPA2 AES найкраща, тому що цей алгоритм використовує великі пакети, рис. 1.

У даному випадку ми бачимо, що найкраще шифрування, це WPA AES та WPA2 TKIP. Найгірший показник має WPA2 AES та WPA TKIP, рис. 2.

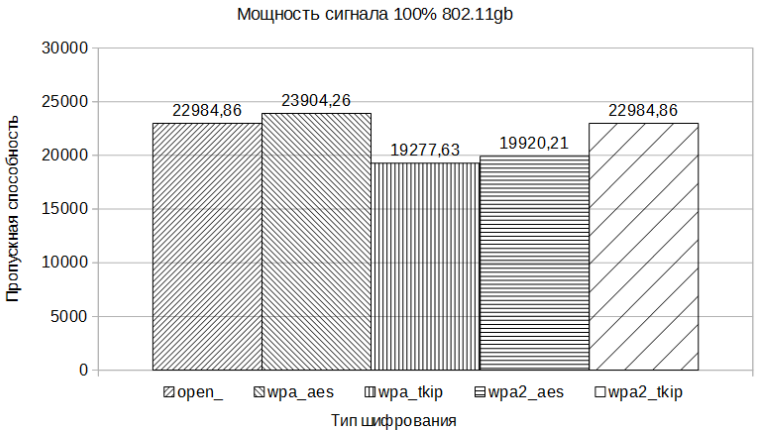

Рисунок 2. Залежність від алгоритму автентифікації та типу шифрування при 100% потужності передачі та протоколі 802.11gb

Найкраще шифрування, це WPA2 AES, а найгірше WPA TKIP, рис. 3.

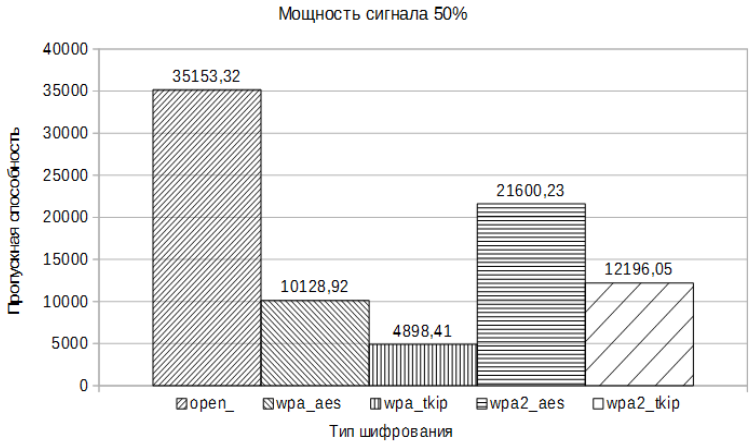

Рисунок 3. Залежність від алгоритму автентифікації та типу шифрування при 50% потужності передачі

Згідно реальним дослідженням було отримано результат, згідно якого у випадку зі 100% потужністю передачі найкраще використовувати тип автентифікації WPA2 AES, у випадку потужності передачі 50% також найкраще використовувати WPA2 AES. У обох випадках найгірші показники отримали, використовуючи тип автентифікації WPA TKIP. Необхідно вибирати тип шифрування в залежності від місця його використання. Якщо

це велика компанія (більше 15 осіб), рекомендується використовувати тип тип автентифікації Enterprise тому, що буде важко кожен раз змінювати пароль для всіх, коли звільниться співробітник. Автентифікацію типу PSK рекомендовано використовувати для меншої групи людей. Згідно з тестами та наявністю атак на шифрування рекомендовано обирати тип автентифікації WPA2 AES тому, що воно більш швидке та безпечніше.

Література

1. Всемирной организации здравоохранения (2014) Электромагнитные поля и общественное здравоохранение. За адресом: http://www.who.int/mediacentre/factsheets/fs304/ru/ (13 Листопада 2015)

2. xTechx Новости Высоких Технологий (2011) Wi-Fi стандарт, сети, механизм передачи сигнала. Недостатки, зоны покрытия, скорость передачи данных. Влияние Wi-Fi на здоровье. За адресом: http://www.xtechx.ru/c40-visokotehnologichni-spravochnik-hitech-book/wi-fi-witwork-tecnology/ (13 Листопада 2015)

3. D-LINK (2014) DAP-2310 За адресом: http://dlink.ru/ru/products/2/1480.html (13 Листопада 2015)

4. D-LINK (2014) Пример настройки MultiSSID на DAP-2310, DAP-2360, DAP-2553, DAP-2690 За адресом: http://dlink.ru/ru/faq/336/1552.html (13 Листопада 2015)

5. D-LINK (2014) Используемые инструменты За адресом: http://dlink.ru/tools/ (13 Листопада 2015)

6. Hobbyits (2012) Устройство и принцип работы Wi-Fi сети (преимущества и недостатки. За адресом: http://hobbyits.com/wan-lan-wi-fi/ustrojstvo-i-princip-raboty-wi-fi-seti-preimushhestva-i-nedostatki.html (13 Листопада 2015)

7.Compfixer (2015) Режимы безопасности Wi-Fi: WEP, WPA, WPA2. Что лучше? За адресом: http://compfixer.info/wpa-wep/ (13 Листопада 2015)

8. GetWiFi Интегратор Беспроводных Технологий (2008) БЕЗОПАСНОСТЬ В СЕТЯХ WIFI. WEP, WPA, WPA2 ШИФРОВАНИЕ. За адресом: http://www.getwifi.ru/psecurity.html (13 Листопада 2015)

9. Олифер В. Г. , Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 е.: ил. УДК 004.7(075)

10. Шахнович И. В. Современные технологии беспроводной связи. Издание второе, исправленное и дополненное Москва: Техносфера, 2006. — 288с. ISBN 5-94836-070-9

11. Хабрахабр (2008) Атака на WPA: подробности, автор: galaxy За адресом: http://habrahabr.ru/post/44496/ (13 Листопада 2015)

Анотація

Продемонстровано найбільш популярні протоколи автентифікації та шифрування Wi-Fi мереж, виявлено їх вплив на пропускну здатність, на екологію і які алгоритми шифрування необхідно використовувати в різних мережах. Було продемонстровано реальні дослідження пропускної здатності та висновки до них.

Ключові слова: Wi-Fi, Безпека, Пропускна здатність, Екологія, Автентифікація, Шифрування, Потужність передавача.

Аннотация

Продемонстрированы наиболее популярные протоколы аутентификации и шифрования Wi-Fi сетей, выявлено их влияние на пропускную способность, на экологию и какие алгоритмы шифрования необходимо использовать в различных сетях. Были продемонстрированы реальные исследования пропускной способности и выводы к ним.

Ключевые слова: Wi-Fi, Безопасность, Пропускная способность, Экология, Аутентификация, Шифрование Мощность передатчика.

Abstract

Showcased the most popular authentication protocols and encryption Wi-Fi networks revealed their influence on the bandwidth on the environment and which encryption algorithms to be used in different networks. There were pro-demonstrate real research capacity and outputs to them.

Keywords: Wi-Fi, Security, Capacity, Ecology, Authentication, Encryption transmitter power.

СИНТЕЗ МОДЕЛІ ДІЯЛНКИ МЕРЕЖІ З ПЕРЕВАНТАЖЕННЯМ

Варваров П.О., ст. гр. ТКСз-14м, mr_orange91@mail.ru
ДонНТУ, Красноармейск, Украина

Проблема перевантаження в мережах TCP/IP виникає у разі, коли кількість переданих даних починає наближатися до значення допустимої пропускної спроможності мережі або навіть перевищувати його. Результатом перевантажень у комп'ютерній мережі є високий рівень втрати пакетів, суттєве збільшення часу їх доставки від відправника до одержувача і навіть тимчасова недоступність мережевих ресурсів і сервісів [1].

Одним з місць виникнення перевантаження є вузькі місця мережі, а саме, черги маршрутизатора, що обмежені об’ємом його буферу, та виникають під час суттєвого збільшення обсягу передачі даних по одному мережному каналу (часто через одночасну роботу декількох користувачів) [2].

Є деяка множина комп'ютерів-хостів, що об’єднані локальною високошвидкісною мережею. Вони підключаються до маршрутизатора, що з однієї сторони з'єднаний з локальною мережею, а з іншої – до низькошвидкісного каналу зв'язку.