Литература

1. Raniwala, A. Tzi-cker Chiueh. Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network, 2008

2. Raniwala, A. Architecture and protocols for a high-performance, secure IEEE 802.11-based wireless mesh network, 2009

Анотація

У статті розглянуто основні способи призначення каналів в багатоканальних mesh-мережах, визначено їх переваги, недоліки та напрями їх подальшої оптимізації з метою підвищення пропускної здатності.

Ключові слова: mesh-мережа, канал, пропускна здатність.

Аннотация

В статье рассмотрены основные способы назначения каналов в многоканальных mesh-сетях, определены их преимущества, недостатки и направления их дальнейшей оптимизации с целью повышения пропускной способности.

Ключевые слова: mesh-сеть, канал, пропускная способность.

Abstract

In this article the main methods of channel assignment in multichannel mesh-networks are researched. Their advantages, shortcomings and routes of the further optimization are defined.

Keywords: mesh-network, channel, bandwidth**.**

ЗАХИЩЕНІСТЬ ВІД MITM-АТАК ЯК ЧИННИК РОЗВИТКУ БЕЗПЕКИ БЛИЖНЬОГО БЕЗКОНТАКТНОГО ЗВ'ЯЗКУ

Якименко С.І.

Науковий керівник — Воропаєва В.Я., к.т.н., доц., проф. каф. АТ

Донецький національний технічний університет,

м. Красноармійськ, Україна

Безконтактні транзакції стають все більш актуальними і поступово замінюють пластикові карти. Наприклад, з 2014 року почався спад показника середньої кількості карт, що припадає на одного українця. Однією з причин скорочення є поява в Україні нового способу розрахунків, здатних забезпечити оперативність і простоту здійснення транзакцій — безконтактних платежів NFC.

NFC (Near Field Communication) — це стандартизована технологія безпровідного зв'язку малого радіусу дії, яка використовує індуктивний зв'язок для обміну даними між електронними пристроями, що знаходяться у безпосередній близькості. Технологія NFC дозволяє користувачам здійснювати прості безконтактні транзакції, діставати доступ до цифрового ко-

нтенту і здійснювати обмін інформацією між пристроями, просто піднося-чи їх один до одного [1].

NFC — це порівняно нова технологія, і тому вітчизняних наукових досліджень щодо її впровадження та систем захисту досі не було. Крім цього, питання безпеки технології NFC — серйозний бар'єр на шляху її просування. Тому задачею статті є, з одного боку, узагальнення зарубіжного досвіду досліджень технології у сфері захисту, з іншого — деякі самостійні кроки, як-от створення моделі специфічного узгодження ключів.

Дійсно, хоча дальність зв'язку NFC обмежена декількома сантиметрами, технологія сама по собі не гарантує безпечний зв’язок.

До загроз, яким можуть піддаватися комунікації ближнього поля, відносять прослуховування, ушкодження і модифікацію даних та «атаку посередника» (man-in-the-middle attack). Розглянемо класичну задачу останньої загрози.

Об'єкт А (Аліса) планує передати об'єкту В (Бобу) деяку інформацію. Об'єкт С (Єва) має відомості про структуру і властивості використовуваного методу передачі даних, а також про факт планованої передачі інформації, яку С планує перехопити. Для здійснення атаки С подає себе об'єкту А як В, а об'єкту В — як А. Об'єкт А, вважаючи, що він направляє інформацію В, посилає її об'єкту С. Об'єкт С, отримавши інформацію і вчинивши з нею деякі дії у своїх цілях, пересилає дані одержувачеві — В; об'єкт В вважає, що інформація була отримана ним безпосередньо від А.

Тепер доведемо, що якщо зв'язок між А і В забезпечується NFC, то реалізувати «атаку посередника» практично неможливо.

Нехай пристрій А працює в активному режимі, а В у пасивному. Аліса генерує радіочастотне поле і відправляє дані Бобу. Єва повинна заважати передачі, щоб Боб не отримав дані. Активний пристрій Аліси на цьому етапі може помітити порушення і зупинити протокол передачі. Якщо цього не сталося, наступним етапом має бути передача Євою повідомлення Бобу. Проблема полягає в тому, що поле, генероване Алісою, є досі там, і Єві треба генерувати інше. Два радіочастотні поля, що є активними одночасно, практично нереально узгодити. Таким чином, практично відсутня можливість того, що Боб зрозуміє дані Єви в активно-пасивному режимі.

Схожим чином твердження доводиться і для активно-активного режиму [2]. Якщо зважити до того ж на малий радіус дії зв’язку, то очевидно, що технологія NFC захищена від «атаки посередника» в практичному використанні.

Саме з цього факту і випливає метод захисту NFC-зв'язку від більшості описаних загроз. Ефективним варіантом є протокол Діффі-Гелмана на еліптичних кривих, за допомогою якого створюється загальний ключ між двома пристроями. Це криптографічний протокол, який захищений від до-

статньої кількості видів витоку інформації, але вразливий до «атак посередника», від яких захищає сама технологія NFC [3, 235]. Загальний секретний ключ може бути використаний для отримання симетричного ключа, який потім використовується для захищеного каналу, що забезпечує конфіденційність, цілісність і достовірність переданих даних.

Протокол Діффі-Гелмана є основою двох з п'яти стандартів захисту NFC від ECMA-International (ECMA-386 и ECMA-409).

Окрім криптографічних, можна створити й специфічну для NFC модель узгодження ключів у стандарті NFC-A. Модель працює при 100%-ній амплітудній модуляції, що забезпечується стандартом в активному режимі. Ідея полягає в тому, що два пристрої відправляють випадкові дані в один і той же час. Пристрої синхронізуються за точним бітовим часом, а також амплітудою і фазою радіочастотного сигналу.

Коли обидва пристрої в один момент посилають випадкові нулі або випадкові одиниці, сумарний сигнал виходить нульовим або подвійним, і зловмисник легко розуміє біти. Значно цікавіше варіант, коли пристрої NFC посилають сигнали різного рівня. Незалежно від того, який з пристроїв (A чи B) подав нульовий рівень напруги, а який — одиничний, зловмисник бачить тільки їх суму і не може відрізнити ці випадки між собою.

Після синхронізації пристрої повинні відкидати всі біти з однаковим значенням або збирати всі біти з різним. Потрібний біт генерується з ймовірністю 50%. Таким чином, генерація 128 біт загального секретного ключа вимагає 256 біт передачі. При швидкості передачі 106 кбіт/с, забезпечуваної стандартом NFC-A, така генерація займає всього 2,4 мс, що є швидким результатом.

Безпека описаного протоколу на практиці залежить від якості синхронізації, що досягається між двома пристроями, якості сигналу, відстані до перехоплювача. Очевидно, що якщо зловмисник може відрізнити дані, відправлені з пристроїв A і B, то протокол порушується. Після того, як відмінності між сигналами від A і B істотно нижче рівня шуму, що отримується перехоплювачем, протокол є безпечним.

Таким чином, у статті розглянута захищеність від «атак посередника» як важливий чинник для захисту NFC від інших загроз. Приведена проста модель специфічного узгодження ключів для NFC в стандарті NFC-A, незалежна від складних криптографічних протоколів. Напрями майбутніх досліджень автора — це розгляд складніших, адаптованих до реальних платіжних систем криптографічних і специфічних алгоритмів; алгоритми токенізації в NFC-платежах; пошук нових загроз, а також вивчення захисту технології від складних атак ретрансляторів (relay attacks).

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-