УДК 004.056.5

Д.І. Прокопович-Ткаченко

Академія митної служби України, Дніпропетровськ

УДОСКОНАЛЕННЯ МЕТОДУ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ БЕЗПРОВОДОВОГО ДОСТУПУ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Пропонується удосконалений метод авторизації та автентифікації безпроводового доступу, який відрізняється від відомих використанням генераторів псевдовипадкових послідовностей максимального періоду, що за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

Ключові слова: *безпека, інформаційна система, безпроводова телекомунікаційна мережа.*

Вступ

Розвиток та вдосконалення телекомунікаційних систем і мереж України здійснюється відповідно до Концепції розвитку телекомунікацій України із застосуванням новітніх технологій, які відповідають міжнародним стандартам, з урахуванням технологічної цілісності всіх мереж та телекомунікаційних засобів, підвищення ефективності та сталості функціонування [1, 2]. Стратегічно важливе значення має забезпечення захисту від несанкціонованого втручання в режими функціонування обладнання телекомунікаційних систем і мереж [3 – 6]. Проведений аналіз [7, 8] показав, що для забезпечення безпеки безпроводових телекомунікаційних систем і мереж застосовуються різні механізми захисту. У теж час [3 – 6] найбільшу загрозу представляють атаки, що спрямовані на порушення роботи протоколів автентифікації і авторизації, а саме уразливості, які пов'язані з невипадковістю генерації ключів авторизації та можливості повторного використання ключів, чий термін життя вже закінчився.

Таким чином, найбільшу небезпеку для протоколів автентифікації та авторизації телекомунікаційних систем та мереж представляють певні недоліки відомих методів і алгоритмів формування ключів авторизації доступу, оскільки на колізійних властивостях цих ключів ґрунтуються всі припущення про безпеку решти механізмів захисту, у тому числі і механізмів шифрування трафіку [9 – 11]. Відповідно до цього актуальною темою дослідження є вдосконалення методів та технічних засобів підвищення безпеки безпроводових телекомунікаційних систем та мереж на основі формування псевдовипадкових ключів авторизації доступу.

Авторизація та автентифікація безпроводового доступу в телекомунікаційних системах, які побудовано за стандартами серії IEEE 802.16

Для формалізованого опису всіх етапів автентифікації та авторизації безпроводового доступу в сучасних телекомунікаційних системах та мережах, які побудовано відповідно до специфікації міжнародних стандартів серії IEEE 802.16, будемо використовувати наступні позначення: pre-PAK – головний ключ авторизації (pre-Primary Authorization Key), який отримано в результаті виконання протоколу автентифікації та авторизації із застосуванням алгоритму RSA; EIK – ключ цілісності (EAP Integrity Key for authenticating Authenticated EAP message), який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для забезпечення цілісності та автентичності переданих даних протоколу EAP; PAK – первинний ключ авторизації (Primary Authorization Key), який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для формування ключа авторизації AK (Authorization Key); MSK – майстер-ключ сеансу (Master Session Key), який формується в процесі автентифікації EAP та призначений для формування парного майстер ключа PMK (Pairwise Master Key); PMK – парний майстер-ключ, який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для формування ключа авторизації AK; Dot16KDF – спеціальна функція, яка призначена для для формування псевдовипадкових послідовностей, які використовуються у якості ключів різного призначення, в тому числі, і для формування ключа авторизації AK; SSID – ідентифікатор мобільної станції, для якої виконана автентифікація EAP; BSID – ідентифікатор базової станції; AK – ключ авторизації, який надає права авторизованого доступу та із застосуванням якого формується решта ключів, в тому числі ключів шифрування трафіку TEK (Traffic Encryption Key).

Основною функцією, яка застосовується під час формування ключів авторизації, є спеціальна функція

Dot16KDF(key, astring, keylength),

аргументами якої є наступні значення:

– key – секретний ключ, який ініціює функцію Dot-16KDF, тобто задає конкретне правило її обчислення;

– astring – значення, яке подається на вхід функції Dot16KDF у якості відкритого параметру, тобто параметру, на який не накладається вимога секретності;

– keylength – несекретний параметр, який визначає бітову довжину виходу перетворення, тобто бітову довжину значення функції Dot16KDF за введеними key та astring.

Конкретна реалізація обчислення функції Dot16KDF залежить від певних налаштувань і може бути побудована одним із сучасних криптографічних алгоритмів. Зокрема, за специфікацією протоколів безпеки стандартів серії IEEE 802.16 у якості базового криптографічного алгоритму пропонується використовувати блокове симетричне шифрування AES (наприклад, в режимі CMAC), алгоритм якого стандартизовано в федеральному стандарті США FIPS-197. Допускається також застосування алгоритму ключового ґешування HMAC із використанням стандартизованої функції SHA.

При авторизації із використанням алгоритму RSA правило формування ключів цілісності EIK та первинних ключів авторизації PAK із застосуванням спеціальної функції Dot16KDF за визначеними (наперед заданими) ідентифікаторами мобільної та базової станції та головним ключем авторизації pre-PAK задається наступним математичним виразом:

$$EIK \mid PAK = Dot16KDF(pre\text{-}PAK, SSID \mid BSID \mid \text{“EIK+PAK”}, 320), \quad (1)$$

де x | y – є конкатенацією бітових послідовностей x та y, тобто, якщо бітову довжину keylength значення функції Dot16KDF задано у 320 бітів, тоді бітові довжини ключа цілісності EIK та первинного ключа авторизації PAK дорівнюють 160 бітів кожна.

При застосуванні для авторизації алгоритму RSA правило формування ключів авторизації безпроводового доступу визначається за наступним виразом:

$$AK = Dot16KDF (PAK, SSID \mid BSID \mid \text{“AK”}, 160). \quad (2)$$

При авторизації із використанням алгоритму EAP правило формування ключів цілісності EIK та парних майстер ключів із застосуванням функції Dot16KDF за визначеними (наперед заданими) ідентифікаторами мобільної та базової станції та майстер-ключем сеансу MSK задається наступним математичним виразом:

$$EIK \mid PMK = truncate (MSK, 320). \quad (3)$$

Наступний вираз задає правило формування ключів авторизації безпроводового доступу із використанням алгоритму EAP:

$$AK = Dot16KDF(PMK, SSID \mid BSID \mid \text{“AK”}, 160). \quad (4)$$

При сумісному використанні RSA і EAP проводяться обидві процедури авторизації, які описані вище. За допомогою pre-PAK також створюється 160-бітовий ключ EIK для автентифікації повідомлень EAP. В результаті АС володіє як PAK, так і PMK, з яких за допомогою функції Dot16KDF генерується AK.

$$AK = Dot16KDF (PAK \oplus PMK, SSID \mid BSID \mid \text{“AK”}, 160). \quad (5)$$

Проведені дослідження дозволяють обґрунтувати наступні вимоги до схеми формування ключів авторизації доступу [8]:

– вхідні послідовності (наприклад, головні ключі авторизації та/або майстер-ключі сеансу), які використовуються у якості векторів ініціації функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) не повинні мати колізій (збігів), тобто схема їх вводу повинна передбачати певний контроль;

– реалізація функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) повинна забезпечувати максимальний період формованих послідовностей.

Виконання сформульованих вимог дозволить забезпечити потрібні ймовірнісно-часові показники формованих ключів авторизації доступу для підвищення безпеки безпроводових телекомунікаційних систем і технологій. Навпаки, невиконання сформульованих вимог гарантовано призведе до колізії (збігу) формованих ключів авторизації доступу із зниженням рівня забезпечуваної безпеки, так як це створює передумови для порушення авторизації безпроводового доступу.

В роботі пропонується удосконалений метод авторизації та автентифікації безпроводового доступу, який відрізняється від відомих використанням генераторів псевдовипадкових послідовностей максимального періоду, що за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

Розробка удосконаленого методу авторизації та автентифікації безпроводового доступу

У якості основи при розробці удосконаленого методу авторизації та автентифікації безпроводового доступу використано відомий метод, який полягає в комплексному застосуванні процедур та операцій організаційного та технічного характеру із створення встановленого режиму авторизації та автентифікації для підвищення безпеки телекомунікаційних систем та мереж.

Основним відмінним елементом удосконаленого методу є застосування генераторів псевдовипадкових послідовностей максимального періоду для формування ключів авторизації доступу, тобто замість спеціальної функції Dot16KDF, колізійні властивості якої є незадовільними, пропонується використовувати більш досконалу функцію генерації послідовностей. Застосування генераторів псевдовипадкових послідовностей максимального періоду за рахунок за-

безпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

Структурна схема удосконаленого методу представлена на рис. 1, на якому наведено сукупність процедур і функцій відомого методу та введені нові елементи, які виділені жирним шрифтом.

Удосконалений метод авторизації та автентифікації безпроводового доступу складається з визначених (рис. 1):

– процедур та операцій передачі даних, які будуються із використанням методів та засобів телепередачі даних і стандартизованих телекомунікаційних протоколів;

– процедур та операцій організації безпечних з'єднань, які будуються із використанням методів та засобів симетричної криптографії та певних механізмів забезпечення безпечного з'єднання, які налаштовуються, зокрема, за встановленим криптографічним комплексом, із визначеними векторами ініціації, секретними ключами та часом їх життя;

– процедур та операцій організації автентифікації користувачів та пристроїв, які будуються із використанням методів та засобів асиметричної криптографії, інфраструктури відкритих ключів, цифрових сертифікатів, тощо, та відповідних протоколів автентифікації та авторизації, зокрема RSA-авторизації, EAP-авторизації та сумісної RSA-EAP-авторизації;

– процедур та операцій формування ключів авторизації доступу, які будуються із використанням методів та засобів (генераторів) псевдовипадкових послідовностей із застосуванням удосконалених механізмів, а саме: процедур контролю векторів ініціації для виконання першої сформульованої вимоги щодо відсутності колізій (збігів) в вхідних послідовностях; безпечних генераторів послідовностей максимального періоду для виконання другої сформульованої вимоги щодо періодичних властивостей ключів авторизації.

Рис. 1. Структурна схема удосконаленого методу авторизації та автентифікації безпроводового доступу для підвищення безпеки телекомунікаційних систем та мереж

Запропоновані процедури контролю векторів ініціації реалізуються шляхом введення до функції генерації ключів авторизації доступу додаткового параметра і (аргументу функції генерації), який визначається за порядковим номером ключа авторизації. Таким чином, для кожного наступного виклику функції генерації використовується унікальний номер, що і забезпечує виконання першої вимоги стосовно відсутності колізій (збігів) в вхідних послідовностях.

При застосуванні для авторизації алгоритму RSA правило формування ключів авторизації безпроводового доступу пропонується визначати як:

AK = Generator (Hash (PAK | SSID | BSID), i, 160), (6)

де Generator(x, y, z) – функція формування псевдовипадкових послідовностей максимального періоду яку ініційовано вектором x та яка повертає y-й блок вихідної послідовності довжини z біт;

Hash (x) – функція безпечного ґешування вектору x;

i – порядковий номер ключа авторизації, тобто номер виклику функції Generator(x, y, z) для заданих (встановлених) SSID та BSID.

Правило формування ключів авторизації безпроводового доступу із використанням алгоритму EAP пропонується визначати за наступним виразом:

AK = Generator (Hash (PMK | SSID | BSID), i, 160). (7)

При сумісному використанні RSA і EAP авторизації правило формування ключів AK пропонується визначати за наступним виразом:

AK = Generator (Hash (PAK | PMK | SSID | BSID), i, 160). (8)

Удосконалений метод авторизації та автентифікації безпроводового доступу відрізняється від відомих, перш за все, використанням генераторів псевдовипадкових послідовностей максимального періоду (додатково введена функція Generator(x, y, z)). Це дозволяє за рахунок забезпечення потрібних колізійних властивостей формованих послідовностей позбавитися збігів ключів авторизації і шляхом зменшення ймовірності збігів до нижньої межі $P_З = 2^{-n}$, де n – бітова довжина формованих ключів авторизації, підвищити безпеку телекомунікаційних систем та мереж.

Перспективним напрямком подальших досліджень є аналіз відомих методів формування псевдовипадкових послідовностей та обґрунтування шляхів побудови безпечних генераторів із забезпеченням максимального періоду формованих ключів авторизації доступу.

Висновки

Проведені дослідження дозволили обґрунтувати наступні вимоги до схеми формування ключів авторизації доступу: вхідні послідовності (наприклад, головні ключі авторизації та/або майстер-ключі сеансу), які використовуються у якості векторів ініціації функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) не повинні мати колізій (збігів), тобто схема їх вводу повинна передбачати певний контроль колізій; реалізація функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) повинна забезпечувати максимальний період формованих послідовностей. В роботі запропоновано удосконалений метод авторизації та автентифікації безпроводового доступу, який відрізняється від відомих використанням генераторів псевдовипадкових послідовностей максимального періоду, що за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволяє підвищити безпеку телекомунікаційних систем та мереж.

Перспективним напрямком подальших досліджень є аналіз відомих методів формування псевдовипадкових послідовностей та обґрунтування шляхів побудови безпечних генераторів із забезпеченням максимального періоду формованих ключів авторизації доступу.

Список літератури

1. Закон України "Про телекомунікації" від 18 листопада 2003 р. N 1280-IV.

2. Концепція розвитку телекомунікацій в Україні, схвалена розпорядженням Кабінету Міністрів України від 7 червня 2006 р. N 316-р.

3. S. Adibi, G.B. Agnew, T. Tofigh, End-to-End (E2E) Security Approach in WiMAX: Security Technical Overview for Corporate Multimedia Applications, 747-758, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

4. S. Adibi, B. Lin, P.-H. Ho, G.B. Agnew, S. Erfani, Authentication Authorization and Accounting (AAA) Schemes in WiMAX, University of Waterloo, Broadband Communication Research Centre (BBCR) , appears in: Electro/information Technology, 2006 IEEE International Conference on 7-10 on pages: 210-215, May 2006.

5. Airspan, "Mobile WiMAX security", Airspan Networks Inc. 2007. [Online]. Available: http:// www.airspan.com.

6. Taeshik Shon and Wook Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", Lecture Notes in Computer Science, vol. 4658, pp. 88-97, Aug. 2007.

7. Прокопович-Ткаченко Д.І. Дослідження протоколів автентифікації та авторизації доступу в безпроводових телекомунікаційних системах та мережах / Д.І. Прокопович-Ткаченко / Системи озброєння і військова техніка, 2013, № 1(33). – С. 119-122.

8. Прокопович-Ткаченко Д.І. Математична модель авторизації та автентифікації безпроводового доступу в телекомунікаційних системах та мережах / Д.І. Прокопович-Ткаченко// Системи обровки інформації. – Х.: ХУПС, 2013. – Вип. 5(112). – С. 111-118.

9. Рашич А.В. Сети беспроводного доступа WiMAX: учеб. пособие / Рашич А.В. – СПб.: Изд-во Политехн. ун-та, 2011. – 179 с.

10. Стандарт беспроводных сетей городского масштаба. — IEEE Std 802.16™–2009.

11. Standard for local and metropolitan area networks. – IEEE Std 802.16m-2011. – 2011.

Надійшла до редколегії 26.04.2013

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет радіоелектроніки, Харків.

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА АВТОРИЗАЦИИ И АВТЕНТИФИКАЦИИ БЕЗПРОВОДНОГО ДОСТУПА ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Д.И. Прокопович-Ткаченко

Предлагается усовершенствованный метод авторизации и автентификации беспроводного доступа, который отличается от известных использованием генераторов псевдослучайных последовательностей максимального периода,

что за счет обеспечения нужных коллизионных свойств формуемых ключей авторизации позволяет повысить безопасность телекоммуникационных систем и сетей.

Ключевые слова: *безопасность, информационная система, беспроводная телекоммуникационная сеть.*

IMPROVEMENT OF AUTHORIZING AND AVTENTIFIKACII METHOD OF OFF-WIRE ACCESS FOR SAFETY INCREASE IN TELECOMMUNICATION SYSTEMS AND NETWORKS

D.I. Prokopovich-Tkachenko

The improved method of authorizing and avtentifikation of off-wire access which differs from the generators of pseudocasual sequences of maximal period known the use is offered, that due to providing of necessary collision properties of the mouldable keys of authorizing allows to promote safety of the telecommunication systems and networks.

Keywords: *safety, informative system, off-wire telecommunication network.*