УДК 004.056.5

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НА БАЗІ СТАНДАРТУ WI-FI

Поповська Є.О.
Науковий керівник – доц. Куля Ю.Е.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14,
кафедра Інфокомунікаційної інженерії імені В.В. Поповського,
тел. (067) 573-19-09.

The given work is devoted to the modern methods of protection surveillance systems established based on wireless systems. The subject of the study is the means of protecting the video surveillance system based on Wi-Fi wireless technology. Conducting a comparative analysis of Wi-Fi protocols. The main methods of wireless network encryption RC4, AES analyzed. Security protocols such as WEP, WPA, WPA2, and WPA3 reviewed and analyzed. The main methods of wireless network encryption RC4, AES analyzed.

Сучасні безпровідні локальні мережі (WLAN) є дуже корисними майже скрізь, як-от коледжі, кафе, метро, офісі тощо відповідно до потреб споживачів на прикладі послуг відеоспостереження. Тому, безпека та конфіденційність WLAN з послугами відеоспостереження є дуже важливим фактором. Безпровідні протоколи безпеки WEP, WPA, WPA2, WPA3 застосовуються для забезпечення автентифікації, конфіденційності та цілісності переданих даних [1].

Безпровідні протоколи працюють на канальному рівні та фізичному рівні стеку мережних протоколів. В свою чергу мережні протоколи використовуються для серії 802.11 протоколів безпровідних мереж і надають сучасні послуги, зокрема відеоспостереження.

1. Розповсюдження: передача кадру до певного або всіх місць призначення. 2. Комбінація: підключення від IEEE до інших мереж WLAN.

3. З'єднання: розпізнавання підключення клієнтів через точку доступу. 4. Повторне підключення: перехід між різними точками доступу, коли з'єднання втрачено. 5. Припинення: припинення існуючого зв'язку або підключення. 6. Перевірка: лише авторизовані користувачі отримують доступ до мереж. 7. Деавтентифікація: видалення дійсного користувача. 8. Секретність: ніхто не може бачити особисті дані іншого. 9. MSDU: Кадри даних служби MAC відповідальні за отримання даних від клієнта до кінцевого пункту призначення.

Звісно, що Wired Equivalent Privacy (WEP) є першим стандартом IEEE 802.11, який реалізує найпростіший механізм автентифікації. Шифрування WEP має багато вразливостей, через які атакуючий може повністю відновити ключ після захоплення мінімального мережного трафіку. Механізм автентифікації, розроблений із єдиним статичним ключем, застосовується всіма користувачами. Управляючий доступ до ключів, часта

їх зміна та виявлення порушень практично неможливі. В даний час на злом WEP витрачаються хвилини.

У 2005 році Федеральне бюро розслідувань США зламало WEP за 3 хвилини, використовуючи комбінацію статистичних методів, зосереджених на захоплених унікальних векторах ініціалізації, та атак методом грубої сили за словником для злому 128-бітних ключів WEP.

Протокол автентифікації для безпровідних локальних мереж забезпечує безпеку даних так само, як і в проводових локальних мережах. Він відповідає безпровідним стандартам 802.11. WEP використовує криптографічний алгоритм RC4 для кодування та декодування пакетів. WEP було розроблено для забезпечення конфіденційності, цілісності та автентифікації кадрів. Конфіденційність забезпечує кодування (алгоритм RC4) пакетів. Цілісність забезпечується циклічною перевіркою надмірності (CRC), а автентифікація здійснюється за допомогою спільного ключа, який відомий лише дійсним користувачам мережі.

Метою алгоритму WEP є забезпечення безпеки між кінцевими користувачами безпровідної локальної мережі через радіосигнали.

Слабкі сторони WEP: 1. Розмір IV є коротким і використовується повторно. 2. Уразливість шифрування RC4 через слабкі ключі. Кадри, які закодовані цими ключами, легко зламати. Оскільки перші три байти ключів беруться з IV, який надсилається незашифрованим у кожному пакеті, цією вразливістю можна легко зловживати шляхом пасивної атаки. Для захоплення 104-бітного ключа WEP потрібно прийняти від 2000 до 4000 реальних пакетів, які перехоплюються за дуже короткий проміжок часу. 3. WEP не зупиняє крадіжку фреймів.4. WEP не зупиняє атаки відтворення.

Щоб усунути вразливості WEP, не змінюючи мережних ресурсів, у 2003 році розроблено новий протокол під назвою Wi-Fi Protected Access. WPA використовує два методи, такі як: WPA Personal або WPA-PSK (Pre-Shared Key – спільний ключ) та WPA Enterprise або Commercial.

WPA Personal 1-3 поколінь використовується для невеликого діапазону мереж, наприклад у коледжах, готелях тощо. Ключ автентифікації може бути до 256 біт. На відміну від WEP, це може бути будь-який буквено-цифровий шаблон і використовується лише для узгодження першого сеансу разом із точкою доступу.

Висновки:

Порівняння безпровідних протоколів безпеки WEP та WPA 1-3 поколінь показало ефективність WPA3 покоління в режимах безпеки, алгоритмів шифрування, наявності прямої секретності та розширеної можливостей розмірах ключа.

Список використаних джерел:

1. Technologies Discussed [Електронний ресурс]. – Режим доступу до ресурсу: https://www.versitron.com/blog/hdcvi-vs-hdtvi-vs-hdahd-hdcctv-technologies-discussed.