Підвищення стійкості протоколів автентифікації в комп'ютерних мережах

Пархомов Максим

Актуальність теми

- Захист інформації завжди був однією з пріоритетних ланок досліджень в історії людства
- Інформацію в сучасному суспільстві вважають звичайним товаром, який легко купується та продається
- Інформація має матеріальну цінність, а тому важливо її захистити.

- **Мета дослідження -** покращення показників захисту протоколу автентифікації в бездротовій комп’ютерній мережі**.**
- **Об’єкт дослідження** - процес автентифікації з’єднання в комп’ютерній мережі.
- **Предмет дослідження -** засоби і методи автентифікації користувача в комп’ютерній мережі.

Задачі дослідження

1. Виконати аналіз існуючих методів захисту передачі даних в бездротових комп’ютерних мережах та провести систематизацію одержаних результатів.
2. Вдосконалити існуючий метод автентифікації в бездротовій комп’ютерній мережі.
3. Розробити програмний засіб — реалізацію вдосконаленого методу автентифікації бездротового мережевого з’єднання.

Новизна результатів

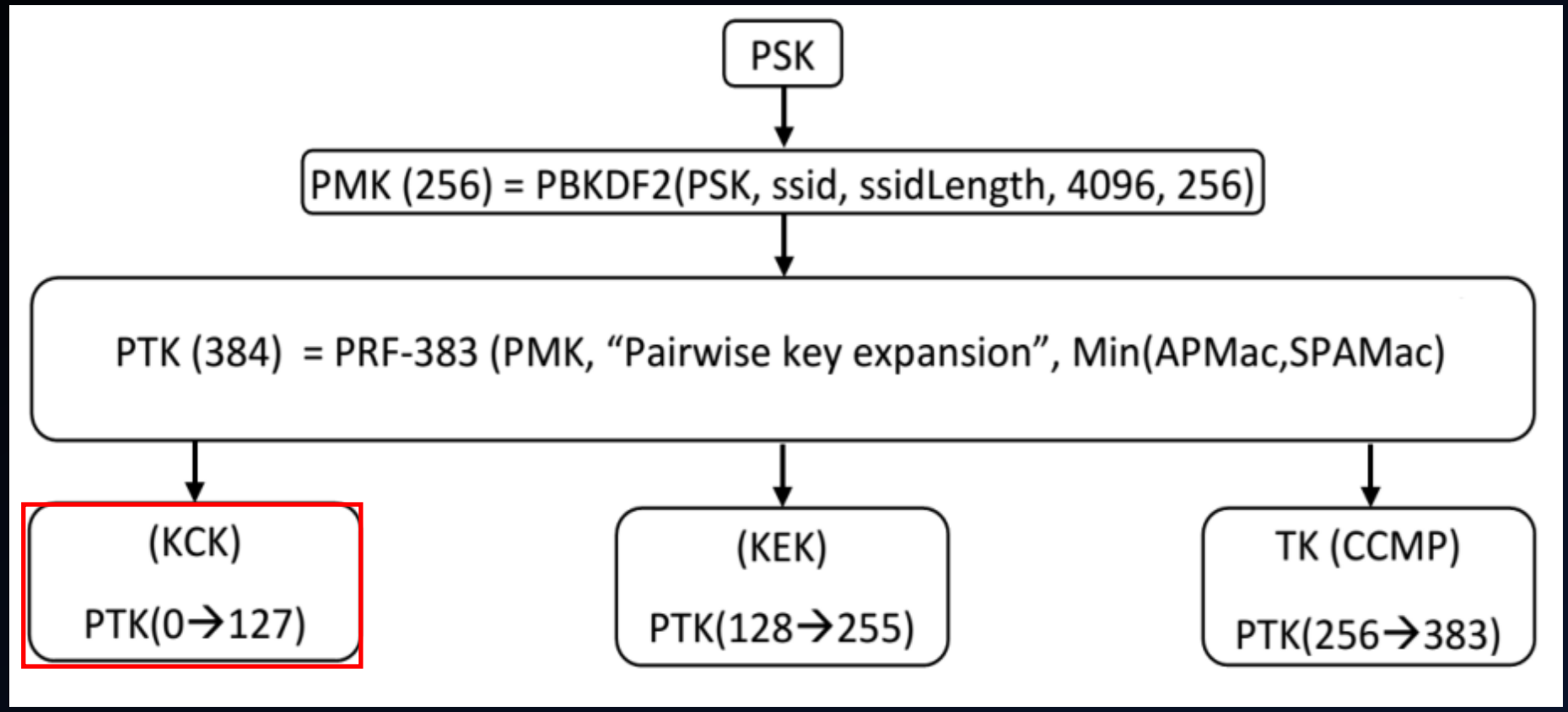
- Модифікований метод автентифікації користувача в бездротовій комп’ютерній мережі за допомогою додаткового шифрування ключа підтвердження, покращило рівень безпеки інформації при використанні бездротових мереж.

Практична цінність

- Розроблений програмний засіб, що створює бездротове з’єднання між комп’ютерами та дозволяє проводити більш захищений обмін інформацією в мережі.

Тип захисту даних у межах стандарту 802.11x	Опис
WEP	«Приватність Рівна Дротовій» це ориганальний стандарт безпеки для бездротових мереж, що легко взламується ПЗ що отримують доступ до мережі після захоплення трафіку
802.1x	Визначає «Розширюваний Протокол Автентифікації» для бездротових мереж, що використовує центральний сервер автентифікації для перевірки кожного користувача. Має відповідні недоліки
LEAP	«Покращений (Легкий) РПА» створений CISCO та базується на EAP та WEP
PEAP	«Захищений протокол РПА» за допомогою якого користувачі мають змогу приєднуватись до серверу без сертифікатів валідності
WPA	«Захищений Бездротовий Доступ» це підвид стандарту безпеки 802.11i та намісник EAP та WEP
TKIP	«Протокол Тимчасової Інтеграції Ключа» є частиною стандарту захисту 802.11i. Він пропонує перемішування ключа за кожним пакетом, повідомлення перевірки цінності та механізми перешифрації
WPA2	Останнє покоління WPA що пропонує підвищений рівень захисту для користувачів мережі

Класифікація існуючих методів захисту даних в межах стандарту 802.11x


PSK
PMK (256) = PBKDF2(PSK, ssid, ssidLength, 4096, 256)
PTK (384) = PRF-383 (PMK, “Pairwise key expansion”, Min(APMac,SPAMac)
(KCK)
PTK(0→127)
(KEK)
PTK(128→255)
TK (CCMP)
PTK(256→383)

Криптостійкість:

$$z = z_h * z_o$$

Практична криптостійкість:

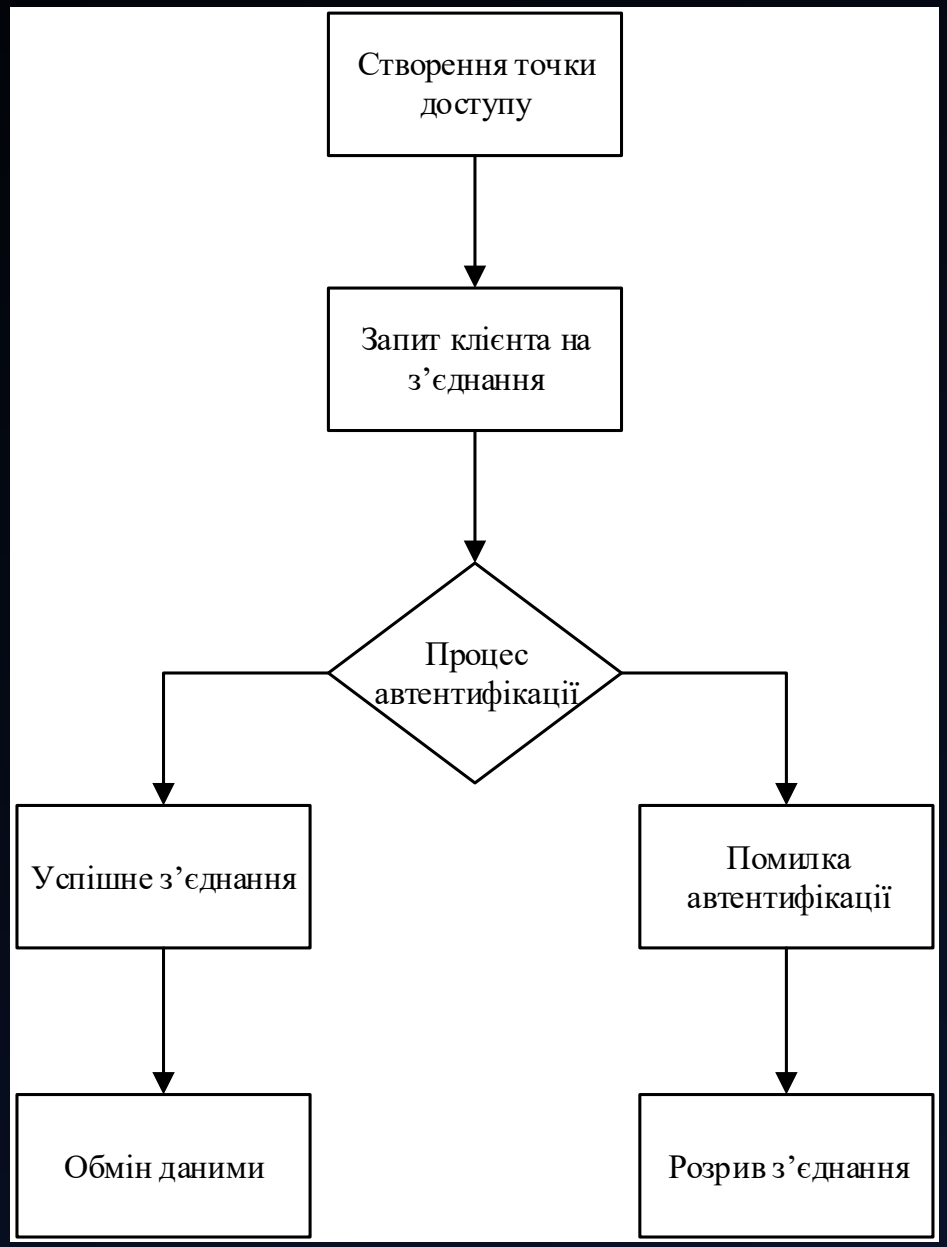
$$К_п = (2^{n_k} * М_{on}) \log_2(М_{mo}(n)).$$

Криптостійкість оригіналу:

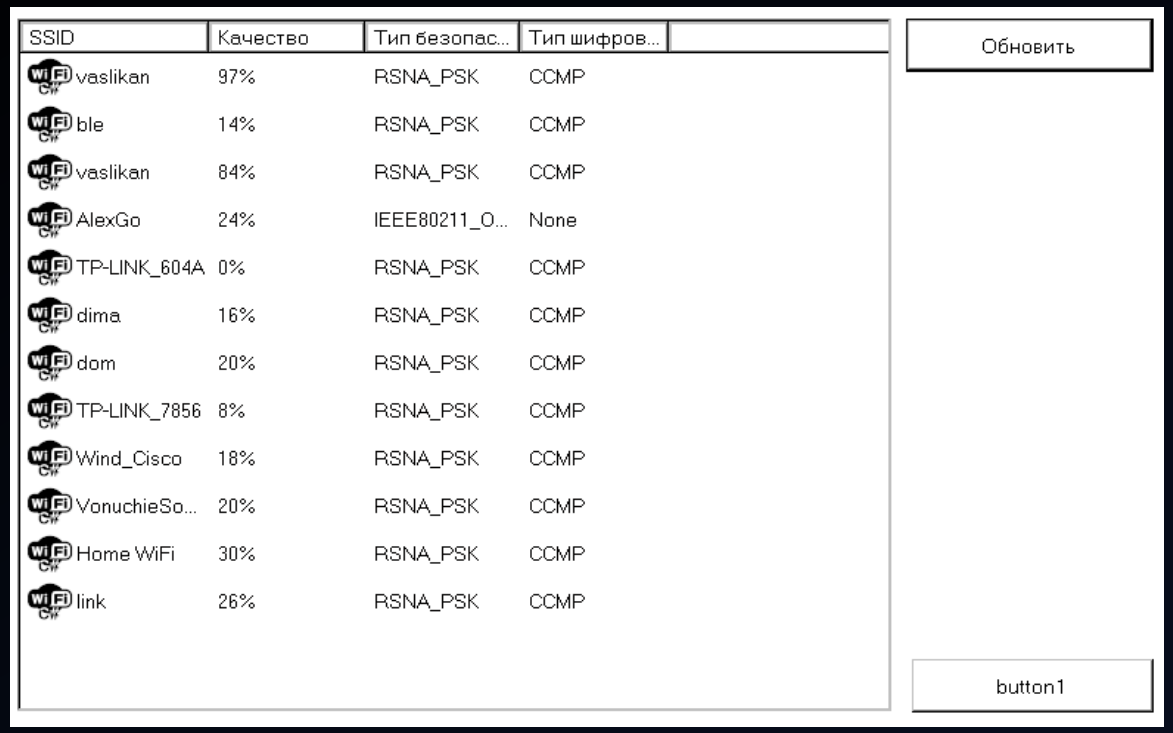
$$К_п = 32 * \log_2 1456 = 336, \text{ отже } z_o = 2^{336}.$$

Криптостійкість покращеного алгоритму:

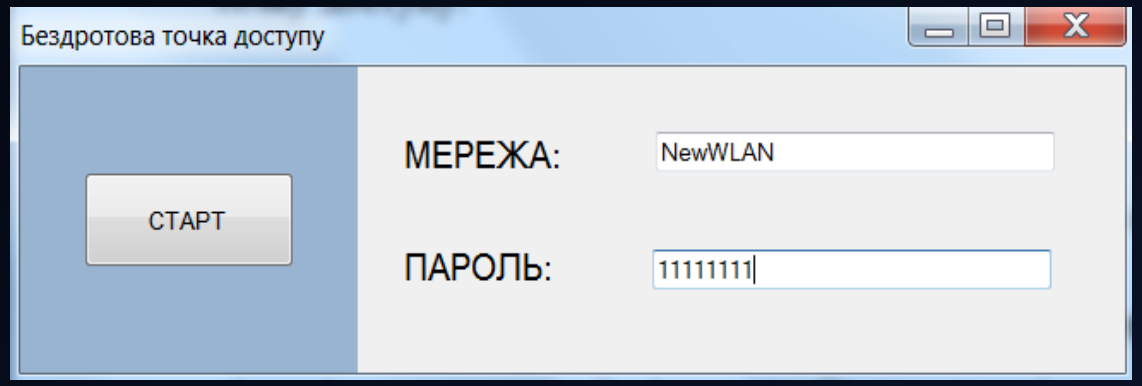
$$К_п = 48 * \log_2 1456 = 504, \text{ отже } z_o = 2^{504}$$



Розроблений алгоритм дії



Вікно серверного додатку



Вікно клієнтського додатку

Економічне обґрунтування

- Аналіз експертних даних показав, що рівень комерційного потенціалу розробки вище середнього
- Загальна вартість витрат на розробку і впровадження складає 56006,32 грн
- Абсолютна ефективність вкладених інвестицій складає 927990,27 грн
- Термін окупності складає 0,62 року

Висновки

- Виконано дослідження актуальних методів захисту мережевого трафіку в бездротових локальних мережах та оброблено отримані результати у вигляді детальних висновків
- Проаналізовано метод захисту мережевої інформації WPA2, визначено переваги його використання у порівнянні з іншими методами захисту
- Розроблено програмний додаток на основі вдосконаленого методу, описано його структуру та метод дії, практичну роботу

ДЯКУЮ ЗА УВАГУ