УДК 004.056
Д.В.Харін
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЇ У WI-FI МЕРЕЖІ (НА ОСНОВІ СТАНДАРТУ IEEE 802.11)

D.V. Harin

RESEARCH OF MECHANISMS OF INFORMATION SECURITY IN A WI-FI NETWORK BASED ON THE STANDARD IEEE 802.11

Надійна система безпеки мережі має ґрунтуватися не на одному методі, а використовувати комплекс засобів захисту. Дієвий захист доступу до Wi-Fi мереж, побудованих на основі стандарту 802.11, можна забезпечити за допомогою засобів Авторизації, Аутентифікації та Аудиту (AAA) з використанням мережевого устаткування Cisco. Засоби AAA підтримують контроль доступу за допомогою локальної бази даних на сервері мережного доступу, або за допомогою віддаленої бази даних захисту, що використовує протоколи захисту AAA [1].

Мережеве устаткування Cisco підтримує три протоколи сервера захисту: TACACS+ (Terminal Access Controller Access Control System - система керування доступом до контролера термінального доступу з поліпшеним використанням сервісів AAA), RADIUS (Remote Access Dial-In User Service - сервіс ідентифікації віддалених абонентів) та Kerberos (Цербер, пропонує механізм взаємної аутентифікації двох співрозмовників (хостів) перед встановленням зв'язку між ними в умовах незахищеного каналу). TACACS+ і RADIUS є головними протоколами сервера захисту, що використовуються для вирішення завдань AAA із серверами, маршрутизаторами та точками доступу. Ці протоколи застосовуються при обміні інформацією про керування доступом між сервером захисту й мережним устаткуванням [1]. Сервери захисту TACACS+ або RADIUS взаємодіють із мережним устаткуванням так, начебто вони є серверами мережного доступу. Сервер мережного доступу виступає в ролі клієнта TACACS+ або RADIUS стосовно сервера захисту TACACS+ або RADIUS. Для обміну інформацією про події AAA між клієнтом і сервером використається протокол TACACS+ або RADIUS. TACACS+ являє собою додаток сервера захисту, що дозволяє на основі відповідного протоколу реалізувати централізоване керування доступом користувачів до сервера мережного доступу, маршрутизатору, Wi-Fi - пристрою або іншому мережному устаткуванню, що підтримує TACACS+. Інформація про сервіси TACACS+ і користувачів зберігається в базі даних, розташовуваної на комп'ютері під керуванням UNIX або Windows NT. TACACS+ дозволяє за допомогою одного сервера керування додатками реалізувати незалежну підтримку сервісів AAA.

RADIUS являє собою розподілений протокол, який використовується у рамках технології клієнт/сервер, що забезпечує захист мережі від несанкціонованого доступу. Cisco підтримує RADIUS як одну зі складових системи захисту AAA. Протокол RADIUS може використовуватися з іншими протоколами захисту AAA, наприклад з TACACS+, Kerberos і локальними базами даних захисту. Варто також відмітити, що для забезпечення безпеки Wi-Fi мереж також використовують різного роду технології обмеження доступу. Найпоширенішими являються фільтрація по MAC-адресах та приховування SSID.

Література

1. Уэнстром М. Организация защиты сетей CISCO. – М.:Вильямс, 2015. – 768 с.