УДК 681.3
Вельмик С. – ст.гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

РЕАЛІЗАЦІЯ ЗАХИЩЕНОГО МЕТОДУ АУТЕНТИФІКАЦІЇ НА ПРИСТРОЯХ WI-FI

Науковий керівник: к.т.н., доцент Мацюк О.В.

Сьогодні постійно росте кількість способів мережного доступу, а злом механізмів захисту та неконтрольований користувальницький доступ є для компаній однією з основних проблем.

Якщо для проникнення у звичайну мережу зловмисникові необхідно фізично до неї підключитися, то у випадку з Wi-Fi всі набагато простіше - потрібно всього лише перебувати в зоні прийому мережі. Крім звичайного доступу до конфіденційних файлів, це може бути розсилання спаму, крадіжка інтернет-трафіку, прослуховування незахищених розмов, зміна та підтасовка даних і т.д.

Враховуючи особливості технології, ефективна система забезпечення безпеки повинна містити в собі кілька компонентів, і головними з них вважаються механізми, які гарантують, що дані дійсно надходять із передбачуваного джерела, а їхній несанкціонований перегляд і зміна неможливі.

Один з методів захисту передачі даних та доступу до мережі Wi-Fi - процес шифрування WEP, який виконується у два етапи. Спочатку підраховується контрольна сума (Integrity Checksum Value - ICV) із застосуванням алгоритму Cyclic Redundancy Check (CRC-32), що додається в кінець незашифрованого повідомлення та служить для перевірки його цілісності прийнятою стороною. На другому етапі здійснюється безпосередньо шифрування. Ключ для WEP-шифрування - загальний секретний ключ, що повинні знати пристрої на обох сторонах бездротового каналу передачі даних. Цей секретний 40-бітний ключ разом з випадковим 24-бітним вектор ініціалізації є вхідною послідовністю для генератора псевдовипадкових чисел, що базується на шифрі Вернама для генерації рядка випадкових символів, називаної ключовим потоком (key stream). Дана операція виконується з метою запобігання методів злому, заснованих на статистичних властивостях відкритого тексту.

Реалізація засобів захищеної аутентифікації, авторизації та аудиту реалізована за допомогою програмного продукту Cisco Secure Access Control Server. Встановлюємо на ПК Cisco Secure ACS, виконуэмо вхід на нього за допомогою будь-якого браузера (Internet Explorer 5 та вище, Opera, Mozilla та ін.), в рядку адреси вводемо http://ip_address_ACS:2002 , де ip_address_ACS - IP-адреса серверу на який було встановлено CS ACS. Після вдалої аутентифікації на сервері, сервер автоматично переадресує на сторінку управлянні сервером через веб-інтерфейс, при цьому буде автоматично змінено номер порту, по якому працює сервер.

Література:

1. “Cisco IOS Software Configuration Guide for Cisco Aironet Access Points”, 2005, электронный ресурс на www.cisco.com.
2. «Администрирование информационно-вычислительных сетей», Н. Т. Кустов, учебное пособие, Томск 2004