УДК 621.391

В.С. Бєлов [1]
О.С. Клімов [1]

ОСНОВИ БЕЗПЕКИ В WI-FI МЕРЕЖАХ

[1]Вінницький національний технічний університет

Анотація.
Приведені основні методи захисту Wi-Fi мереж та їх вразливості.
Ключові слова: Wi-Fi, підключення, шифрування, аутентифікація, безпека.

Abstract.
The basic methods of protecting Wi-Fi networks and their vulnerabilities are given.
Keywords: *Wi-Fi, connectivity, encryption, authentication, security.*

Вступ

Як і будь-яка комп'ютерна мережа, Wi-Fi – є джерелом підвищеного ризику несанкціонованого доступу. Крім того, проникнути в бездротову мережу значно простіше, ніж в звичайну, непотрібно підключатися до проводів, досить опинитися в зоні прийому сигналу.

Звичайний користувач може буквально за декілька хвилин налаштувати домашню мережу, але, не маючи базових знань про ці технології та забезпечення безпеки в локальній мережі,він стає легкою мішенню для того, хто хоче проникнути в його мережу. І, якщо дехто може сказати, що йому нема чого приховувати на своєму комп‘ютері, то він не усвідомлює того факту, що хакер може використати його комп‘ютер для здійснення своїх атак

Основна частина

Основним методом є використання непомітного ім'я мережі (SSID). Ідентифікатор службового набору SSID - це один із основних налаштувань мережі Wi-Fi. Хоча не схоже на те, що ім'я мережі може скомпрометувати безпеку, але, безумовно, може. Використання занадто загальний ідентифікатор SSID, як "бездротовий" або ім'я постачальника за умовчанням, може полегшити коректному режимі захисту WPA або WPA2. Це відбувається тому, що алгоритм шифрування містить SSID, а словники, що розбивають паролі, що використовують хакери, попередньо завантажуються з загальними та типовими SSID. Використання одного з них просто полегшує роботу хакера.

Хоча це може мати сенс називати SSID чимось легко ідентифікувати, як-от назву компанії, адресу або номер набору, що, можливо, також не найкраща ідея. Це особливо вірно, якщо мережа знаходиться в спільній будівлі або в безпосередній близькості від інших будівель або мереж. Якщо хакери їздять через перевантажену зону та бачать дюжину різних мереж Wi-Fi, вони, швидше за все, націлюватимуть на найпростіший для ідентифікації, що може допомогти їм зрозуміти, що вони можуть отримати, взламуючи його. Вони також можуть вибрати один, який простіше знайти в перевантаженій області.

У разі прихованого SSID поле порожнє, тобто виявлення бездротової мережі є неможливим і не можна до неї підключитися, не знаючи значення SSID. Але всі станції в мережі, які підключені до точки доступу, знають SSID і під час підключення, коли розсилають Probe Request запити, вказують ідентифікатори мереж, наявні в їх профілях підключень. Прослуховуючи робочий трафік, з легкістю можна отримати значення SSID, необхідне для підключення до бажаної точки доступу.

Також слід пам’ятати про фізичну безпеку. Бездротова безпека - або вся IT-безпека може мати бездогані технології та протоколи. Ви можете мати найкраще шифрування і всеодно бути вразливим. Фізична безпека - одна з цих вразливостей. Потрібно пам’ятати що доступ до Wi-Fi можливий за допомогою фізичного втручання.

У більшості точок доступу є кнопка скидання, яку хтось може натиснути, щоб відновити заводські настройки за умовчанням, видалити безпеку Wi-Fi і дозволити будь-кому підключитися. Таким чином, Wi-Fi , що поширюються по всій вашої установі, також має бути фізично захищений, щоб уникнути втручання. Переконайтеся, що вони завжди недоступні, і розгляньте можливість використання будь-

яких механізмів блокування, запропонованих продавцем роутера, для фізичного обмеження доступу до кнопок та портів AP.

Ще однією проблемою фізичної безпеки, пов'язаної з Wi-Fi, є те, що хтось додає неавторизований роутер до мережі, яка зазвичай називається "недобросовісною версією". Це може звісно бути зроблено на законних підставах працівника, який бажає додати більше охоплення Wi-Fi. Щоб запобігти таким типам шахраїв, гарантуйте, що всі невикористовувані порти Ethernet (наприклад, стінні або вихідні мережі) вимикаються. Ви можете фізично видалити порти або кабелі або вимкнути зв'язок цього розетки або кабелю з маршрутизатором або вимикачем. Або якщо ви дійсно хочете підвищити безпеку, увімкніть аутентифікацію 802.1X на дротовій стороні, якщо ваш маршрутизатор або комутатор підтримують це, так що будь-який пристрій, що підключається до мереж Ethernet, повинен ввести вхідні дані для доступу до мережі.

Ще одним ефективним з методів є використання Enterprise WPA2 з аутентифікацією 802.1X. Цей метод найефективніших механізмів захисту Wi-Fi, який ви можете встановити - це розгортання корпоративного режиму безпеки Wi-Fi, оскільки він аутентифікує кожного користувача індивідуально: кожен може мати власне ім'я користувача та пароль Wi-Fi. Тому, якщо ноутбук або мобільний пристрій загублено, викрадено, або працівник залишає компанію, все, що вам потрібно - це змінити або скасувати реєстрацію конкретного користувача.

За допомогою корпоративної Wi-Fi безпеки користувачі вводять своє унікальне ім'я користувача та пароль під час підключення.

Іншою великою перевагою режиму підприємства є те, що кожному користувачеві присвоюється його власний ключ шифрування. Це означає, що користувачі можуть лише розшифрувати трафік даних для власного з'єднання - не спостерігаючи за чисельним іншим трафіком бездротового зв'язку.

Щоб поставити свій ПП в режим підприємства, вам спочатку потрібно буде налаштувати сервер RADIUS. Це дає можливість аутентифікації користувача та підключається до бази даних або каталогу (наприклад, Active Directory), яка містить всі імена користувачів і паролі.

Хоча Ви могли б розгорнути індивідуальний сервер RADIUS, спочатку перевірте, чи ваші інші сервери (наприклад, Windows Server) вже надають цю функцію. Якщо ні, розгляньте службу RADIUS на основі хмарної або розміщеної служби. Також майте на увазі, що деякі точки доступу до бездротового доступу або контролери забезпечують базовий вбудований сервер RADIUS, але їх межі продуктивності та обмежені функції зазвичай роблять їх корисними тільки для малих мереж.

Приклад того, як ви налаштовували AP, використовуючи IP-адресу, порт та секретний сервер RADIUS.

Захист налаштування клієнта 802.1X. Як і в інших технологіях безпеки, корпоративний режим роботи Wi-Fi безпеки все ще має деякі вразливості. Один з них - атака "людина з середини", з хакером сидячим в аеропорту чи кафе, або навіть на стоянці корпоративного офісу. Хтось міг створити підроблену мережу Wi-Fi з таким самим або схожим SSID, як і мережа, яку вони намагаються скопіювати. І в певний момент коли Ваш ноутбук або пристрій намагатиметься підключитися, RADIUS-сервер зловмисника може захопити ваші реєстраційні дані. Потім він може використовувати Ваші реєстраційні дані для підключення до реальної мережі Wi-Fi.

Спосіб запобігти таким атакам це провести аутентифікацію 802.1X - це перевірка сервера на стороні клієнта. Коли безпроводовий клієнт увімкнув перевірку сервера, клієнт не передаватиме ваші облікові дані для входу Wi-Fi на сервер RADIUS, доки він не підтвердить, що він підтримує зв'язок із зареєстрованим сервером. Точні можливості перевірки сервера та вимоги, які ви можете накласти на клієнтів, будуть відрізнятися залежно від пристрою або ОС клієнта.

Наприклад, у Windows можна ввести доменні імена зареєстрованого сервера, вибрати сертифікат, який видав сертифікат сервера, а потім вимкнути нові сервери або сертифікати. Отже, якщо хтось налаштував підроблену мережу Wi-Fi та сервер RADIUS, і ви спробуєте увійти до нього, Windows зупинить це підключення.

Ви знайшли функцію підтвердження сервера 802.1X у Windows при налаштуванні параметрів EAP з'єднання Wi-Fi.

Одним важливим аспектом є виявлення Rogue-AP або запобігання безпровідному втручанню. Ми вже торкнулися трьох сценаріїв уразливих точок доступу: там, де зловмисник може встановити підроблену мережу Wi-Fi та сервер RADIUS, інший, де хтось може скинути AP до заводських налаштувань, і третій сценарій, за допомогою якого хтось може підключити їх власний AP.

Кожен із цих неавторизованих ЗП може тривалий час залишатись непоміченими для IT-персоналу, якщо не буде встановлено відповідний захист. Таким чином, гарна ідея - увімкнути будь-який тип виявлення викрадень, який пропонує ваш постачальник послуг AP або бездротового контролера. Точний метод виявлення та функціональність змінюються, але більшість з них, принаймні, періодично

скануватимуть ефір і надсилатимуть вам сповіщення, якщо новий АР визначено в межах допустимих точок доступу.

Більше можливостей для розпізнавання деяких постачальників ПЗ пропонують повноцінну систему виявлення бездротового втручання (WIDS) або систему захисту від вторгнення (WIPS), яка може відчувати безліч безпровідних атак та підозрілу активність разом із нелюдськими ПП. До них відносяться помилкові запити на деаутентифікацію, запити про помилки асоціації та підробку MAC-адреси.

Крім того, якщо це справжній захист WIPS, а не WIDS - це просто виявити, оскільки він повинен мати змогу приймати автоматичні контрзаходи, такі як від'єднання або блокування підозрілого безпроводового клієнта для захисту від атаки мережі.

Якщо Ваш постачальник послуг АР не надає вбудоване виявлення антивірусом програмне забезпечення або WIPS, розгляньте стороннє рішення. Ви можете подивитися на сенсорні рішення, які зможуть відслідковувати як продуктивність Wi-Fi, так і проблеми безпеки, від компаній, таких як 7SIGNAL , Cape Networks та NetBeez .

Висновки

Таким чином, основними аспектами безпеки мереж Wi-Fi є маскування SSID, використання індивідуальної ідентифікації за допомогою Enterprise WPA2 секретний сервер RADIUS, а також виявлення Rogue-AP на основі технологій виявлення бездротового втручання (WIDS) або системи захисту від вторгнення (WIPS). Також важливо дотримуватись корпоративних правли безпеки, що виключить, або значно зменшить вплив людського фактору.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пролетарский А.В., Баскаков И.В., Чирков Д.Н. «Беспроводные сети Wi-Fi». - М:БИНОМ. Лаборатория знаний, 2007,-178 с.
2. Щербаков В.Б., Ермаков С.А. «Безопасность беспроводных сетей: стандарт IEEE 802.11». - М: РадиоСофт, 2010, -255 с.
3. 5 Ways to Secure Wi-Fi Networks // Network World - Режим доступу: https://www.networkworld.com/article/3224539/mobile-wireless/5-ways-to-secure-wi-fi-networks.html
4. Бєлов В.С. Архітектура мереж WI-MAX / В.С. Бєлов, О.І. Мельничук // Конференції ВНТУ електронні наукові видання, XLVI Науково-технічна конференція факультету інфокомунікацій, радіоелектроніки та наносистем (2017). – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/2563
5. Палагнюк Д.М. Еволюція стандартів IEEE802.11x / Д.М. Палагнюк, В.С. Бєлов // Конференції ВНТУ електронні наукові видання, XLVI Науково-технічна конференція факультету інфокомунікацій, радіоелектроніки та наносистем (2017). – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/2569
6. Кичак В.М. Оцінка впливу кількісних характеристик зміни інформаційного параметру на завадостійкість каналів зв'язку з КАМн / В.М. Кичак, В.С. Бєлов, А.С. Бєлов. // Науковий журнал «Вісник Хмельницького національного університету». – 2012. - №4.- с. 59-62

Бєлов Володимир Сергійович **–** асистент кафедри телекомунікаційних систем і телебачення, Вінницький національний технічний університет, м. Вінниця, e-mail: belov@vntu.edu.ua

Клімов Олександр Сергійович **–** студент групи ТКТ-16мс, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, м. Вінниця, e-mail: sashava103@gmail.com.

Belov Vladimir – assistant of the Chair of Telecommunication Systems and Television, Vinnytsia National Technical University. Vinnitsa, e-mail: belov@vntu.edu.ua

Klimov Oleksandr - group TKT-16ms, The Faculty of Infocommunications, Radioelectronics and Nanosystems, Vinnytsia National Technical University, Vinnitsia, e-mail: sashava103@gmail.com.