5. Захожай О.І. Основні аспекти структурної організації комбінованих систем розпізнавання образів / О.І. Захожай, Ю.Е. Паеранд // Вестник ХНТУ №1 (44). – Херсон: «Олди-Плюс». – 2012 – С. 221 – 225.

ВРАЗЛИВОСТІ WI-FI МЕРЕЖ

Білевська О. С.
науковий співробітник
Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
м. Київ, Україна

Радіоканал передачі даних, який використовується в Wi-Fi мережах, потенційно схильний до втручанню з метою порушення конфіденційності, цілісності і доступності інформації. При підключенні до мережі передбачена аутентифікація та шифрування, але ці елементи захисту мають свої вади.

Шифрування значно знижує швидкість передачі даних, і, найчастіше, воно усвідомлено відключається адміністратором для оптимізації трафіку. Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований за рахунок вразливостей в алгоритмі розподілу ключів RC4 (Rivest Cipher 4). Стандарт WPA2 представляє собою покращений WPA. Основна відмінність між WPA і WPA2 полягає в технології шифрування, який поєднує симетричний алгоритм блочного шифрування AES (Advanced Encryption Standart) та TKIP. WPA2 забезпечує більш високий рівень захисту мережі, так як TKIP дозволяє створювати ключі довжиною до 128 біт, а AES – до 256 біт.

Більшість атак починаються з розвідки, під час якої виконується сканування мережі, збір і аналіз пакетів. Багато службових пакетів в мережі Wi-Fi передаються у відкритому вигляді. При цьому вкрай проблематично з'ясувати, хто легальний користувач, який намагається підключитися до мережі, а хто збирає інформацію. Після розвідки приймаються рішення про подальші кроки можливої атаки.

Найбільш поширеними є два технічних сценаріїв атак на мережі Wi-Fi – це перехоплення пакетів, які пов'язані з аутентифікацією клієнта (рукостискання – handshake) з подальшим перебором пароля за словником, і створення підробленої точки доступу з паралельним проведенням атаки «відмови в обслуговуванні» на справжню точку доступу.

Для шифрування переданих даних в мережі Wi-Fi в основному використовується алгоритм WPA2 з відключеною технологією WPS. На даний час алгоритм WPA2 є найбільш розповсюдженим алгоритмом захисту бездротових мереж.

Найбільш розповсюджена атака на мережу Wi-Fi, захищеної протоколами WPA-PSK або WPA2-PSK – це атака за словником. Протокол захисту WPA-PSK або WPA2-PSK використовує ключ попередньої сесії (PTK – Pairwise Transient Key), який в свою чергу складається з попереднього загального ключа (PSK – Pre-Shared Key) та п'яти інших параметрів, таких як SSID (символьна назва бездротової точки доступу Wi-Fi), Authenticator Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адреса точки доступу) та Suppliant MAC-address (MAC-адреса wifi-клієнта). Цей ключ в подальшому використовує шифрування між точкою доступу і клієнтом. Зловмисник, який прослуховує ефір, може перехопити усі п'ять параметрів окрім PSK. PSK отримується завдяки використанню парольної фрази WPA-PSK, яку відправляє користувач разом із SSID. Комбінація цих двох параметрів пересилається за стандартом формування ключа на основі пароля PBKDF2 (Password Based Key Derivation Function), який генерує 256-бітовый загальний ключ. В звичайній WPA-PSK/WPA2-PSK атаці за словником зловмисник може використовувати програмне забезпечення, яке виводить 256-бітний PSK для кожної парольної фрази і використовувати її з іншими параметрами, які були описані в створенні PTK. PTK буде використовуватися для перевірки контрольної суми (MIC – Message Integrity Check) в одному з пакетів handshake. Якщо вони співпадуть, то парольна фраза в словнику буде вірною. При цьому використовуються вразливості протоколу аутентифікації користувачів – відкрита передача ANounce, SNounce, MAC-адреси точки доступу і MAC-адреси WiFi-клієнта. Якщо при відтворенні алгоритму аутентифікації відбудеться успішна авторизація користувача, значить обраний зі словника пароль є істинним і атака призвела до успішного злому мережі.

В 2018 році створено новий стандарту безпеки – WPA3. Творці WPA3 спробували усунути концептуальні недоробки, які випливли з появою атаки KRACK. Оскільки ключова вразливість ховалася в чотирьохелементному рукостисканні, у стандарт WPA3 додалася обов'язкова підтримка більш надійного методу з'єднання – SEA (Simultaneous Authentication of Equals), також відомого як Dragonfly. Технологія SEA заснована на протоколі обміну ключами Діффі–Хеллмана з використанням кінцевих циклічних груп. SEA надає інтерактивний метод, у відповідності з яким дві і більше сторін встановлюють криптографічні ключі, які засновані на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який отримує кожна зі сторін для

аутентифікації з'єднання, обирається на основі інформації з пароля, ключів і MAC-адрес обох сторін. Якщо ключ однієї зі сторін виявиться скомпрометованим, це не спричинить компрометації ключа сесії. І навіть дізнавшись пароль, атакуючий не зможе розшифрувати пакети.

Ще одним нововведенням WPA3 є підтримка захисту керуючих пакетів PMF (Protected Management Frames) для контролю цілісності трафіку.

Однак протокол WPA3 має і два типи недоліків. Перший призводить до атак з зниженням рейтингу, а другий – до витоків бічного кеша. Алгоритм кодування пароля в Dragonfly, містить умовні гілки. Якщо зловмисник може визначити, яка гілка ланцюга «if-then-else» була вилучена, він може дізнатися, чи був знайдений елемент пароля в конкретній ітерації цього алгоритму. В основі атаки по бічному каналу на основі синхронізації, лежить атака на метод рукостискання Dragonfly. Цей метод використовує певні мультиплікативні групи, алгоритм кодування пароля використовує змінне число ітерацій для кодування пароля. Точна кількість ітерацій залежить від пароля, який використовується, і MAC-адреси точки доступу і клієнта. Зловмисник може виконати віддалену тимчасову атаку на алгоритм кодування пароля, щоб визначити скільки ітерацій знадобилося для кодування пароля. Відновлена інформація може бути використана для виконання парольної атаки, яка схожа на автономну атаку за словником.

Висновки.

З огляду на вищевикладене для захисту Wi-Fi мереж необхідно впроваджувати комплексний підхід до забезпечення інформаційної безпеки. Необхідно приділяти увагу підвищенню обізнаності співробітників в питаннях інформаційної безпеки та перекривати потенційні вектори атак на мережу. Впроваджувати безпечні методи аутентифікації з перевіркою сертифікатів, обмежувати доступ клієнтів гостьової мережі до локальної обчислювальної мережі, проводити регулярний аналіз захищеності бездротових мереж, виявляти і відключати несанкціоновані точки доступу.

Література:

1. Mathy Vanhoef, Eyal Ronen, Dragonblood. Analysing WPA3's Dragonfly Handshake, [Електронний ресурс]. – Режим доступу: http://wpa3.mathyvanhoeF. com
2. Stewart S. Miller, Wi-Fi Security –McGraw-Hill Networking Professional Publishing, 2003, 309p.