МОДЕЛЬ RD-АТАКИ

Вацлавик Олег

Львівський державний університет безпеки життєдіяльності, Львів, Україна

Summary. Considerations of RD attacks on implanted medical devices at emergency states of the patient. Consider a new scheme based on the patient's access template to the implanted medical device and uses a vector support machine.

Keywords: information security, RD attacks, implanted medical device, authentication.

Через обмежені ресурси ІМП у термінах споживаної потужності , продуктивності процесора та об'єму пам'яті є досить складно розробити ефективну схему контролю доступу до ІМП.

В ідеальному випадку ІМП повинен би взаємодіяти лише з невеликою кількістю зчитувачів (таких як зчитувач вдома у пацієнта чи кабінеті лікаря). Більше того , комунікація не повинна відбуватися в будь-який час. Для більшості пацієнтів доступ до ІМП демонструє певний тип шаблону. Базуючись на цьому спостереженні , можна побудувати модель нормального доступу пацієнта до ІМП, яка тоді може бути використана для виявлення спроб шкідливого доступу шляхом поєднання моделі та ефективного класифікую чого алгоритму. Якщо ІМП виявляє спробу шкідливого доступу він переходить в режим сну та зберігає енергію. Така схема уникає втрат енергії під час процесу автентифікації, а отже ефективно захищає від RD-атак.

Розглянемо нову схему , яка базується на шаблоні доступу пацієнта до ІМП та використовує Векторизовану машину підтримки (ВМП). В ній використовується мобільний телефон пацієнта для виконання більшості обчислень. Ця схема є першою лінією захисту. Тобто вона запускається перед будь-якою процедурою автентифікації . Якщо будь-яка спроба доступу не пройде нашу схему, автентифікація не здійснюватиметься. Це збереже значну кількість енергії пристрою . Якщо зчитувач пройде нашу схему, далі потрібно буде пройти автентифікацію , яка забезпечує додатковий захист доступу до ІМП.

RD-атака розглядається як атака примусової автентифікації. ІМП взаємодіє через безпровідний канал з зовнішнім зчитувачем. Якщо автентифікацію не пройдено, тоді ІМП розриває взаємодію з зчитувачем. Проте процес автентифікації сам по собі вимагає від ІМП виконання багатьох обчислень та передач іформації , що споживають значну частку енергії. Якщо неавторизований зчитувач постійно намагається з'єднатися з ІМП , це спричиняє виконання ІМП багатьох автентифікацій , що споживає значну частку ємності батареї. На додаток до цього , цей тип атак генерує масив записів про події безпеки , які заносяться в журнал, що також є RD-атакою на ємність пам'яті ІМП.

Атаки примусової автентифікації можуть бути легко здійснені зловмисником через використання технології SDR (Software-Defined Radio) програмно-заданої радіо технології (рис. 1).

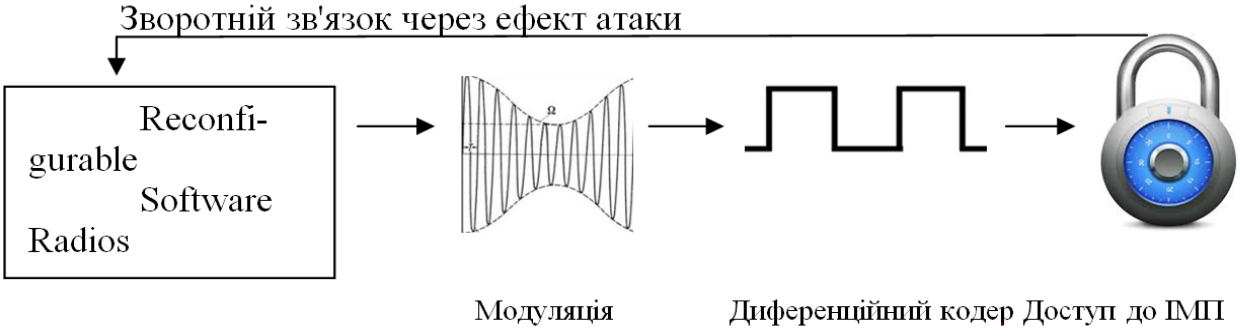

Рис. 1. Атака на ІМП з допомогою SDR

SDR – радіо-телекомунікаційна система , яка може бути налаштована на довільну смугу частот та приймати різні види модульованого сигналу і яка складається з програмованого обладнання з програмним керуванням. SDR виконує значну частину цифрової обробки сигналів на звичайному ПК або на ПЛІС. Метою таких систем , є радіоприймач або радіопередавач довільних радіосистем , який налаштовується шляхом програмної переконфігурації.

Через такі RD-атаки зловмисник може наносити безпосередню шкоду пацієнту розряджаючи джерело енергії ІМП. RD-атаки можуть зменшити ефективний час життя ІМП з декількох років до декількох тижнів, роблячи ІМП некорисним , та створюючи загрозу здоров'ю пацієнта. Тому критично важливим є розроблення легковагових та ефективних схем захисту для ІМП , які можуть протидіяти RD-атаці.

Література

1. В. В. Марков. Хакерські атаки на імплантати як один із способів протиправного використання кіберпростору: сутність та види.
2. Яцишин М. Ю. Актуальні проблеми захисту прав людини у кіберпросторі.
3. Орленко В. С. Методи оцінки та підвищення захищеності інформаційних ресурсів систем спеціального призначення. Автореф. Дис. На здобуття наук. Ступеня к.т.н.: 05.13.21 "Системи захисту інформації", Київ, 2009 (ДСК).
4. Avant 4000 bluetooth wireless oximetry: increased safety and accuracy when administering the six-minute walk test, Nonin Medical, Inc., Technical Report, 2008
5. X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks on implantable medical devices. inProceedings of the IEEE Globecom 2010, 2010, pp.1-5
6. K. Malasri, L. Wang, Securing wireless implantable devices for healthcare: ideas and challenges. IEEE Commun.47, 74-80 (2009)